

TITLE OF THE INVENTION

System for Preventing Unauthorized Use of Recording Media

This application is based on an application No. 2002-208398 filed in Japan, the content of which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

(1) Field of the Invention

The present invention relates to a technology for preventing unauthorized use of a recording medium which is mountable to a terminal device.

(2) Related Art

In recent years, a system has been proposed that enables users to access information recorded on a recording medium with use of a terminal device to which the recording medium is mountable, such as a portable telephone.

The reference 1 discloses a system that includes a smart card and a portable terminal device. Here, the smart card stores thereon user information and information relating to applications to be used, and the portable terminal device is equipped with an authentication unit that authenticates whether the user is authorized to use the portable terminal device.

In this system, when the smart card is mounted to the

portable terminal device, authentication is performed whether the user is the authorized user, with use of information inputted through the portable terminal device and information that is on the smart card. When the user is authenticated to be the authorized user, the user will be allowed to access information written on the smart card.

However, with the aforementioned technology, the authentication unit within the portable terminal device is not protected against an unauthorized external attack. Therefore, there is a possibility that a malicious third party decodes the authentication unit of the portable terminal, and changes the authentication unit to always authenticate the third party to be the authorized user. Such tampering will allow third parties to access the information recorded on the recording medium.

【Reference 1】

Japanese Laid-open Patent Application 2001-134688

SUMMARY OF THE INVENTION

The object of the present invention is to provide a recording medium that is protected against unauthorized use, that therefore has heightened security, and further to provide a terminal apparatus, a system, a method, and a program, for preventing unauthorized use of the recording medium.

In order to achieve the stated object, the present invention is a portable recording medium that is characterized by including: a storage unit which stores therein storage authentication information that authenticates a user, and has an area that corresponds to the storage authentication information; a judgment unit operable to judge whether to perform authentication; a reception unit operable to receive reception authentication information that authenticates a user, if the judgment unit judges affirmative; an authentication unit that is tamper-resistant and is operable to judge whether the received reception authentication information matches the storage authentication information; and a process unit operable to permit use of the area if the reception authentication information is judged to match the storage authentication information.

According to this structure, the recording medium includes therein an authentication unit that is tamper resistant. Because of being tamper-resistant, the authentication unit will be prevented from being decoded or tampered by third parties. Accordingly, the recording medium enables to prevent third parties from illegally using the area within the recording medium.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In the drawings:

FIG. 1 shows an overall structure of the recording-medium unauthorized use prevention system;

FIG. 2 is a block diagram showing the structure of a portable telephone 100 that relates to the first embodiment;

FIG. 3 is a block diagram showing the structure of a recording medium 300 that relates to the first embodiment;

FIG. 4 shows the data structure of the authentication information table T300 that the first storage area 311 of the first embodiment owns;

FIG. 5 shows the data structure of the process information table T301 that the second storage area 312 of the first embodiment owns;

FIG. 6 is a flowchart showing the operations for setting authentication information and process information, which relate to the first embodiment;

FIG. 7 is a flowchart showing the authentication operation that relates to the first embodiment;

FIG. 8 is a flowchart showing the user information reception operation;

FIG. 9 is a flowchart showing the access right setting operation;

FIG. 10 is a block diagram showing the structure of the portable telephone 100A that relates to the second embodiment;

FIG. 11 is a block diagram showing the structure of the recording medium 300A that relates to the second embodiment;

FIG. 12 shows the data structure of the authentication information table T350 that the first storage area 311A of the second embodiment owns;

FIG. 13 shows the data structure of the communication information table T351 that the third storage area 313A of the second embodiment owns;

FIG. 14 shows the data structure of the process information table T352 that the second storage area 312A of the second embodiment owns;

FIG. 15 is a flowchart showing the operations for setting communication information, authentication information, and process information, which relate to the second embodiment;

FIG. 16 is a flowchart showing the authentication operation that relates to the second embodiment;

FIG. 17 is a flowchart showing the access right setting operation that relates to the second embodiment;

FIG. 18 is a block diagram showing the structure of the portable telephone 100B that relates to the third embodiment;

FIG. 19 is a schematic circuit diagram of the connection

unit 115B that the portable telephone 100B of the third embodiment owns;

FIG. 20 is a block diagram showing the structure of the recording medium 300B that relates to the third embodiment;

FIG. 21 shows the data structure of the history information table T400 that the history information storage area 354B of the third embodiment owns;

FIG. 22 is a flowchart showing the operation for registering history information, which relates to the third embodiment;

FIG. 23 is a flowchart showing the authentication operation that relates to the third embodiment, which continues to FIG. 24;

FIG. 24 is a flowchart showing the authentication operation that relates to the third embodiment, which is a continuation from FIG. 23;

FIG. 25 is a flowchart showing the access right setting operation that relates to the third embodiment;

FIG. 26 shows the data structure of the table consisting of authentication information and process information;

FIG. 27 shows the data structure of a table consisting of authentication information, communication information, and process information, where there is only one piece of communication information; and

FIG. 28 shows the data structure of a table consisting

of authentication information, communication information, and process information, where there are a plurality of pieces of communication information.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. The First Embodiment

As the first embodiment according to the present invention, a recording-medium unauthorized use prevention system 1 is described as follows.

1.1 The structure of the recording-medium unauthorized use prevention system 1

As shown in FIG. 1, the recording-medium unauthorized use prevention system 1 is comprised of portable telephones 100 and 200, an IC-function equipped recording medium 100 and 200, an IC-function equipped recording medium (hereinafter simply "recording medium") 300 to which each portable telephone is mountable.

The recording medium 300 is mounted to a portable telephone 100, for use. Likewise, the recording medium 300 can be mounted to the portable telephone 200, for use.

1.2 The structure of the portable telephone 100

In this section, the structure of the portable telephone 100 is described.

As shown in FIG. 2, the portable telephone 100 is comprised of an output unit 101, an input unit 102, a radio unit 103, a baseband signal process unit 104, a speaker 105, a microphone

106, a fingerprint input unit 107, a control unit 108, an input/output unit 109, and a power supply unit 110.

The portable telephone 100 is specifically a computer system comprised of a microprocessor, a ROM, a RAM, a display unit, and the like. The ROM stores thereon a computer program. The portable telephone 100 pursues its function by the microprocessor performing according to the computer program.

The portable telephone 200 has the same structure as the portable telephone 100, therefore the description thereof is omitted.

(1) The output unit 101

The output unit 101 outputs display of data according to the instruction by the control unit 108.

The output unit 101, upon receiving from the control unit 108 input-means information for inquiring about which input means to be used in authentication in relation to the recording medium 300, outputs a message inquiring about which input means to be used in authentication.

The output unit 101, if it receives from the control unit 108 a character input request, outputs a message prompting the user to input character information. The character input request specifically requests input of character information that is composed of a combination of one or more numbers, alphabets, and signs, and is used for proving that he is the authorized user of the recording medium 300. If the output

unit 101 receives from the control unit 108 a fingerprint input request, it outputs a message prompting the user to input fingerprint information. The fingerprint input request specifically requests input of fingerprint information that exhibits characteristics of the fingerprint of the user, and is used for proving that he is the authorized user of the recording medium 300.

Further, the output unit 101, upon receiving authentication-impossible information showing that there is no information within the recording medium 300 that matches the character information, the fingerprint information, or the combination of character information and fingerprint information, having been received from the input unit 102, outputs a message reporting that there is no matching information within the recording medium 300.

(2) The fingerprint input unit 107

The fingerprint input unit 107 has a fingerprint sensor that reads the fingerprint pattern of the user, generates from the fingerprint pattern fingerprint information composed of characteristic points of the fingerprint pattern, and outputs the generated fingerprint information to the control unit 108.

Here, the characteristic points of the fingerprint pattern are specifically direction and relative position for ending of ridges and bifurcations, and the like.

(3) The input unit 102

The input unit 102 is comprised of a touch panel, a keyboard having ten key input function, and the like, and outputs to the control unit 108 an input instruction from the user, the input instruction including coordinates information showing the location at the touch panel that has been pushed, and a key operation signal generated by a key input through the keyboard.

The input unit 102 receives input of authentication-start information that indicates to start authentication in relation to the recording medium 300, and also receives input of other kinds of information. The input unit 102 outputs the authentication-start information and the other kinds of information to the control unit 108.

The input unit 102, when the output unit 101 outputs a message inquiring about an input means of information that is necessary for authentication, receives one of first input information, second input information, and third input information. The first input information indicates that information necessary for authentication will be input through the input unit 102; the second input information indicates that such information will be input through the fingerprint input unit 107; and the third input information indicates that such information will be input through both of the input unit 102 and the fingerprint input unit 107. The input unit 102 then outputs the received one of the first, second, or third input

information to the control unit 108.

Furthermore, the input unit 102, when the output unit 101 outputs a message prompting the user to input character information, receives the input of such character information which is used for proving that he is the authorized user of the recording medium 300, and outputs the received character information to the control unit 108.

(4) The radio unit 103

The radio unit 103 is equipped with an antenna 120, and transmits/receives radio signals.

(5) The baseband signal process unit 104

The baseband signal process unit 104 processes a signal received from the radio unit 103 to output it to the speaker 105, and processes an audio received from the microphone 106 to output it to the radio unit 103.

(6) The speaker 105

The speaker 105 outputs the audio processed at the baseband signal process unit 104.

(7) The microphone 106

The microphone 106 receives an audio of the user, and outputs the audio to the baseband signal process unit 104.

(8) The control unit 108

The control unit 108 controls the portable telephone 100 as a whole.

The control unit 108, upon receiving authentication-start

information or other kinds of information from the input unit 102, outputs the authentication-start information or the other kinds of information to the recording medium 300 via the input/output unit 109. Further, the control unit 108, upon receiving the input-means information from the recording medium 300 via the input/output unit 109, outputs the received input-means information to the output unit 101.

Furthermore, the control unit 108, when it receives from the input unit 102, one of the first, second, and third input information, outputs the received one of the first, second, and third input information, to the recording medium 300 via the input/output unit 109. The control unit 108, upon receiving from the recording medium 300 either a character input request or a fingerprint input request, outputs the received one of the character input request and the fingerprint input request to the output unit 101.

The control unit 108 receives character information or fingerprint information, which identifies the user, and outputs the received one of the character information and fingerprint information, to the recording medium 300 via the input/output unit 109. Further, the control unit 108, upon receiving authentication-impossible information from the recording medium 300, outputs the received authentication-impossible information to the output unit 101.

The control unit 108 owns a memory, which is operable

to store data and program, the data including input instructions received from the input unit 102 and content which has been processed by the control unit 108, and the program including a variety of process programs and a variety of application programs that are to be executed. The control unit 108, when using data of the recording medium 300, receives the data from the recording medium 300, and records the received data to this memory.

For example, when there is, via the input unit 102, an instruction from a user that a game stored in the recording medium 300 should be executed, the control unit 108 receives data necessary for execution of the game from the recording medium 300, records it on the memory, and executes the game processing with use of the recorded data.

(9) The input/output unit 109

The input/output unit 109 performs input/output of information with the recording medium 300, after the recording medium 300 has been inserted to a slot provided for the portable telephone 100, and with use of the slot as an interface.

(10) The power supply unit 110

The power supply unit 110 supplies power voltage to each part constituting the portable telephone 100, and to the recording medium 300.

1.3 The structure of the recording medium 300

In this section, the structure of the recording medium

300 is described.

As shown in FIG. 3, the recording medium 300 is comprised of a storage area 310, a control unit 320, a setting unit 330, and an input/output unit 340.

The recording medium 300 is specifically a computer system which is comprised of a microprocessor, a ROM, a RAM, and the like. The ROM stores thereon a computer program. The recording medium 300 pursues its function by the microprocessor performing according to the computer program.

(1) The storage area 310

The storage area 310 includes a first storage area 311, a second storage area 312, and a process-name storage area 315. The storage area 310 further includes a memory A 361, a memory B 362, and a game 363, which are respectively data accessible to a user. Note here that the memory A 361, the memory B 362, and the game 363 have been prestored in the recording medium 300 before purchase.

(a) The first storage area 311

The first storage area 311 has an authentication information table T300, one example of which is shown in FIG. 4.

This authentication information table T300 stores thereon at least one set of authentication number and authentication information.

The authentication number is a number assigned to each

piece of authentication information.

The authentication information is for identifying the authorized user of the recording medium 300, which is necessary for judging whether to allow access to the recording medium. The authentication information is specifically one of character information, fingerprint information, and a combination of character information and fingerprint information.

It should be noted here that "N.A." in FIG. 4 represents that the authentication information is not necessary. Hereinafter, the authentication number that corresponds to the authentication information of "N.A." is referred to as "authentication-unnecessary number".

(b) The second storage area 312

The second storage area 312 has a process-information table T301, one example of which is shown in FIG. 5.

The process-information table T301 stores thereon at least one set of process number and process information.

The process number is a number assigned to each piece of process information.

The process information shows a name of a process which becomes accessible after authentication.

An authentication number and the corresponding process number are assigned a same number, so as to associate the authentication information and the corresponding process information.

The process names registered in the process information include such as "memory A", "memory B", that each correspond to the names of the memory A 361 and the memory B 362, and "game" that corresponds to the name of the game 363. If "memory A" has been registered as the process name, such processes are enabled as referring to, changing, and deleting the content of the data files within the memory A 361, and registering a new data file to the memory A 361. The same thing as the aforementioned case of "memory A" applies to the case in which "memory B" has been registered.

If "game" has been registered, it enables use of program data and data files necessary for the execution of the game 363. The game is executed by using these program data and data files.

(c) The process-name storage area 315

The process-name storage area 315 store thereon process-in-use information identifying the process names of processes that are currently made accessible after the authentication was performed in relation to the recording medium 300.

Please note here that, after the purchase of the recording medium 300 and until the first authentication is performed, no process-in-use information is stored in the process-name storage area 315.

(2) The setting unit 330

The setting unit 330 is tamper-resistant, and includes therein an authentication-information setting unit 331 and a process-information setting unit 332.

(a) The authentication-information setting unit 331

As described as follows, the authentication-information setting unit 331 registers authentication information received through an external terminal, into the first storage area 311, either at the time when the recording medium 300 is purchased or at the time when it is commenced to be used. Here, the external terminal is a terminal located at a sales office selling the recording medium 300.

The authentication-information setting unit 331 receives, as authentication information, one of character information, fingerprint information, and a combination of character information and fingerprint information, that is to be registered into the first storage area 311 from the external terminal via the input/output unit 340, then judges whether the received authentication information has been registered in the authentication information table T300. If the authentication information has not been registered, the authentication-information setting unit 331 calculates an authentication number for the authentication information to be registered, and registers the authentication information with the calculated authentication number into the authentication information table T300 of the first storage area

311. Note here that the authentication-information setting unit 331 temporarily stores the calculated authentication number for the process-information setting unit 332 to be able to refer to.

Please note that judgment whether the received authentication information has been already registered in the authentication information table T300 is performed as follows.

That is, if the received authentication information consists of only character information, judgment is performed by searching for information matching the received character information within the authentication information table T300.

If the received authentication information consists of only fingerprint information, judgment is performed by searching for information matching the received fingerprint information within the authentication information table T300. Here, the information matching the received fingerprint information is information that matches 80% or more of the characteristic points of the fingerprint pattern that the received fingerprint information possesses.

If the received authentication information consists of both of character information and fingerprint information, judgment is performed by searching for information matching both of the character information and the fingerprint information, within the authentication information table T300. Here, the information matching both of the character information

and the fingerprint information is information that perfectly matches the received character information, and that matches 80% or more of the characteristic points of the fingerprint pattern that the received fingerprint information possesses.

(b) The process-information setting unit 332

As described as follows, the process-information setting unit 332 registers process information received through the external terminal into the second storage area 312, either at the time when the recording medium 300 is purchased, or at the time when it is commenced to be used.

The process-information setting unit 332 receives process information to be registered to the second storage area 312, from the input/output unit 340 via the control unit 320, and acquires the value of the temporarily stored authentication number as process number. The process-information setting unit 332 then registers the acquired process number and the received process information into the process information table T301 of the second storage area 312, and the data relating to the acquired process information to the storage area 310. In registration, the process-information setting unit 332 sets the process for the process name to be registered to a state in which it is impossible to be used.

By the above operations, the authentication information and the process information are associated with each other.

(3) The control unit 320

The control unit 320 is tamper-resistant, and includes therein an authentication unit 321 and a process unit 322.

The control unit 320 receives authentication-start information and other kinds of information, from the portable telephone 100 via the input/output unit 340. Upon receiving information from the portable telephone 100, the control unit 320 judges whether the received information is authentication-start information or not. If judging that it is authentication-start information, the control unit 320 outputs the received authentication-start information to the authentication unit 321, and makes the authentication unit 321 start authentication. If the received information is judged not to be authentication-start information, authentication will not be performed.

(a) The authentication unit 321

The authentication unit 321, upon receiving authentication-start information from the control unit 320, outputs input-means information to the portable telephone 100 via the input/output unit 340.

The authentication unit 321, if receiving first input information from the portable telephone 100 via the input/output unit 340, outputs a character input request to the portable telephone 100 via the input/output unit 340, then receives character information from the portable telephone 100 via the input/output unit 340.

The authentication unit 321, if receiving second input information from the portable telephone 100 via the input/output unit 340, outputs a fingerprint input request to the portable telephone 100 via the input/output unit 340, then receives fingerprint information from the portable telephone 100 via the input/output unit 340.

The authentication unit 321, if receiving third input information from the portable telephone 100 via the input/output unit 340, first outputs a character input request to the portable telephone 100 via the input/output unit 340, and receives character information from the portable telephone 100 via the input/output unit 340. Next, the authentication unit 321 outputs a fingerprint input request to the portable telephone 100 via the input/output unit 340, and receives fingerprint information from the portable telephone 100 via the input/output unit 340.

The authentication unit 321 receives, from the portable telephone 100 via the input/output unit 340, one of character information, fingerprint information, and a combination of character information and fingerprint information identifying the user. Then the authentication unit 321 performs authentication by judging whether authentication information matching the received information exists within the authentication information table T300.

If receiving character information, the authentication

unit 321 judges whether authentication information matching the received character information exists in the authentication information table T300. Here, the authentication information matching the received character information is authentication information that perfectly matches the received character information.

If receiving fingerprint information, the authentication unit 321 judges whether authentication information matching the received fingerprint information exists in the authentication information table T300. Here, the authentication information matching the received fingerprint information is authentication information that matches 80% or more of the characteristic points of the fingerprint pattern that the received fingerprint information possesses.

If receiving both of character information and fingerprint information, the authentication unit 321 judges whether authentication information matching both of the character information and the fingerprint information exists in the authentication information table T300. Here, the authentication information matching both of the character information and the fingerprint information is authentication information that perfectly matches the received character information, and that matches 80% or more of the characteristic points of the fingerprint pattern that the received fingerprint information possesses.

Please note that information received from the portable

telephone 100 at the time of authentication is hereinafter referred to as "user information." This user information is information that identifies a user, and is represented by one of character information, fingerprint information, and a combination of character information and fingerprint information.

If authentication information matching the received user information exists in the authentication information table T300, the authentication unit 321 acquires the authentication number of the authentication information and outputs it to the process unit 322.

If authentication information matching the received user information does not exist in the authentication information table T300, the authentication unit 321 generates authentication-impossible information and outputs it to the portable telephone 100 via the input/output unit 340. If the authentication information table T300 has information whose authentication information is "N.A.", the corresponding authentication number is acquired and outputted to the process unit 322.

Please note here that, if only character information is received, the authentication information matching the received user information is authentication information that matches the received character information; and if only fingerprint information is received, it is authentication information that

matches the received fingerprint information; and if both of character information and fingerprint information are received, it is authentication information that matches both of the character information and the authentication information that have been received.

(b) The process unit 322

The process unit 322 receives an authentication number from the authentication unit 321.

In the meantime, the process unit 322 judges whether the process-name storage area 315 stores thereon process-in-use information. If judging affirmative, the process unit 322 reads the process-in-use information from the process-name storage area 315, to acquire the name of the process that is permitted for use. Then the process unit 322 sets access right so that the process corresponding to the acquired process name is inaccessible.

Further, the process unit 322 acquires from the process information table T301 process information corresponding to the process number that matches the received authentication number, and sets access right so that the process for the process name registered in the acquired process information is accessible. Further, the process unit 322 updates the process-name storage area 315 so that the process-in-use information is replaced by the process name registered in the acquired process information.

For example, if the process name registered in the acquired process information is "game", access right is set so that only "game" is accessible for execution.

By the above operation, only a process for the process name that corresponds to the authentication information is enabled to be used.

After the authentication and while the portable telephone performs the process set to be accessible, the process unit 322 performs control between the portable telephone 100 and the process set to be accessible, by performing read/write of data to/from the process set to be accessible.

(4) The input/output unit 340

The input/output unit 340 receives information either from the portable telephone 100 or from an external terminal, and according to the content of the received information, outputs it either to the control unit 320, or to the setting unit 330 via the control unit 320.

The input/output unit 340 also receives information from the control unit 320, and outputs the received information to the portable telephone 100.

1.4. The operations of the recording-medium unauthorized use prevention system 1

In this section, each operation of the recording-medium unauthorized use prevention system 1 is described.

(1) The setting operations for authentication information

and process information

Here, the operations for setting authentication information and process information are described with reference to the flowchart of FIG. 6.

The authentication-information setting unit 331 receives, from the input/output unit 340, authentication information having been inputted from the external device (Step S1). Then it judges whether the received authentication information has been already registered in the authentication information table T300 (Step S3). If the authentication information has been already registered, the operation ends. If it has not been registered yet, the authentication-information setting unit 331 calculates an authentication number with use of the authentication information table T300, registers the calculated authentication number and the received authentication information in the authentication information table T300 of the first storage area 311, and also temporarily stores thereon the authentication number for the process-information setting unit 332 to be able to refer to (Step S5).

The process-information setting unit 332 receives, from the input/output unit 340, process information having been inputted from the external device, and sets the temporarily stored authentication number to be the process number, registers the process number and the received process information in the process information table T301, and sets the process whose

process name has just been registered, to be inaccessible (Step S10).

Note here that the process information registered at Step S10 may be process information unregistered in the process information table T301, and also may be process information already registered in the process information table T301.

(2) The authentication operation

Here, the authentication operation is described with reference to the flowchart shown in FIG. 7.

The control unit 320 receives information from the portable telephone 100 (Step S45), and judges whether the received information is authentication-start information or not (Step S48). If it is judged not to be authentication-start information, authentication will not be performed. If it is judged to be authentication-start information, the control unit 320 outputs the authentication-start information to the authentication unit 321 (Step S50). Upon receiving the authentication-start information from the control unit 320, the authentication unit 321 outputs input-means information to the portable telephone 100, and receives, from the portable telephone 100, one of first input information, second input information, and third input information (Step S51). The authentication unit 321 performs operation for receiving user information (Step S52).

Next, the authentication unit 321 judges whether

authentication information that matches the received user information exists in the authentication information table T300 (Step S55).

If such authentication information matching the received user information exists, the authentication unit 321 acquires the authentication number that corresponds to the authentication information from the authentication information table T300, and outputs the acquired authentication number to the process unit 322 (Step S60). The process unit 322 performs operation for setting access right (Step S65).

If such authentication information matching the received user information does not exist, the authentication unit 321 generates authentication-impossible information, and outputs the generated authentication-impossible information to the portable telephone 100 via the input/output unit 340 (Step S70). Next, the authentication unit 321 judges whether an authentication-unnecessary number exists in the authentication information table T300 (Step S75). If such authentication-unnecessary number exists, the authentication unit 321 acquires the authentication-unnecessary number, and outputs it to the process unit 322 (Step S80). The process unit 322 performs operation for setting access right (Step S83).

If there is no authentication-unnecessary number, the operation ends.

(3) The user information reception operation

Here, the operation for the user information reception process performed at Step S52 of FIG. 7 is described with reference to the flowchart shown in FIG. 8.

The authentication unit 321 judges whether the information received from the portable telephone 100 is first input information or not (Step S85). If the received information is first input information, the authentication unit 321 outputs a character input request to the portable telephone 100, and receives character information from the portable telephone 100 (Step S86). Note here that until character information is received as user information at Step S86, the operation is in a state of waiting to receive character information.

If the received information is not first input information, the authentication unit 321 judges whether it is second input information (Step S87). If the received information is second input information, the authentication unit 321 outputs a fingerprint input request to the portable telephone 100, and receives fingerprint information from the portable telephone 100 (Step S88). Note here that until fingerprint information is received as user information at Step S88, the operation is in a state of waiting to receive fingerprint information.

If the received information is not second input information, the authentication unit 321 outputs a character input request to the portable telephone 100, and receives character information from the portable telephone 100 (Step S89), and

then outputs a fingerprint input request to the portable telephone 100, and receives fingerprint information from the portable telephone 100 (Step S90). Note here that until character information is received at Step S89, the operation is in a state of waiting to receive character information, and that until fingerprint information is received at Step S90, the operation is in a state of waiting to receive fingerprint information.

(4) The access right setting operation

Here, the access right setting operation performed at Step S65 and Step S83 shown in FIG. 7 is described with reference to the flowchart shown in FIG. 9.

The process unit 322 receives an authentication number from the authentication unit 321 (Step S93). Next, the process unit 322 judges whether process-in-use information exists (Step S94).

If process-in-use information exists, the process unit 322 reads the process-in-use information from the process-name storage area 315, acquires the process name of the process that has been made accessible, and sets access right so that the process corresponding to the acquired process name is made inaccessible (Step S95). Further, the process unit 322 acquires from the process information table T301 process information that corresponds to the process number that matches the authentication number received at Step S93, sets access right

to the process corresponding to the process name registered in the acquired process information, so that the process will become accessible (Step S96). The process unit 322 updates the process-in-use information in the process-name storage area 315, with use of the process name registered in the process information acquired at the Step S96 (Step S97).

If process-in-use information does not exist, the operation from Step S96 will be performed.

(5) Examples of authentication operation

Here, a specific flow of the authentication operation is described with reference to each table shown in FIG. 4 and FIG. 5.

The authentication unit 321, upon receiving, from the portable telephone 100, fingerprint information and character information "PW3" as user information, acquires the authentication number "4" from the authentication information table T300. The process unit 322 acquires, from the process information table T301, process information in which "memory A + B" and "game" are registered as process name, with use of the process number "4" that matches the authentication number "4", thereby setting access right to the memory A + B and to the game, so that they become accessible.

When receiving character information "PW2" as user information, the authentication unit 321 makes the memory A and the game accessible.

When receiving character information "PW5" as user information, the authentication unit 321 outputs to the portable telephone 100 a message reporting that there is no authentication information that matches the "PW5" in the authentication information table T300. Then, the authentication unit 321 judges whether authentication-unnecessary number exists in the authentication information table T300. Since this example has an authentication-unnecessary number, the authentication unit 321 acquires "1" which is the authentication-unnecessary number. The process unit 322 acquires, from the process information table T301, process information whose process name registered is "memory A" with use of the process number "1" that corresponds to the authentication number "1", thereby setting such as access right to the memory A, and makes it accessible.

The above operations enable setting of different authentication information to information of different importance levels, by classifying information to the memory A and memory B according to importance level.

1.5 Summary of the first embodiment

As described above, the recording-medium unauthorized use prevention system 1 has, within the recording medium 300, an authentication unit 321 that is tamper-resistant. This makes it difficult for third parties to encode or tamper the authentication system of the authentication unit. Therefore, unauthorized access of third parties to the recording medium

300 is prevented.

In addition, the recording medium 300 stores thereon one or more pieces of authentication information, and further one or more pieces of process information that each correspond to a piece of authentication information. Therefore, the authentication information makes it possible to restrict accessible data, unlike conventionally where one authentication is enough for using all the data stored in the recording medium. By this arrangement, the recording medium 300 has heightened security for the owner.

2. The second embodiment

As the second embodiment according to the present invention, a recording-medium unauthorized use prevention system 2 is described as follows.

2.1 The structure of the recording-medium unauthorized use prevention system 2

The recording-medium unauthorized use prevention system 2 has the same structure as the recording-medium unauthorized use prevention system 1, and is comprised of portable telephones 100A, 200A, and a recording medium 300A to which each portable telephone is mountable.

The recording medium 300A stores thereon at least one piece of communication information that represents a telephone number which is used when the portable telephone 100A is used

as a communication device. The process means is associated with both of the communication information and authentication information.

The portable telephone 100A accepts an input of communication information from the recording medium 300A, and an input of user information, acquires process information that corresponds to both of the accepted communication information and the authentication information that matches the received user information, and permits use of the process name registered in the acquired process information.

The recording medium 300A can be also mounted to the portable telephone 200A, for use.

In this section, the description mainly focuses on the differences with the recording-medium unauthorized use prevention system 1.

2.2 The structure of the portable telephone 100A

In this section, the structure of the portable telephone 100A is described.

Because the portable telephone 100A has a similar structure to the portable telephone 100 of the first embodiment, the difference between them will be mainly described.

As shown in FIG. 10, the portable telephone 100A is comprised of an output unit 101A, an input unit 102A, a radio unit 103A, a baseband signal process unit 104A, a speaker 105A, a microphone 106A, a fingerprint input unit 107A, a control

unit 108A, an input/output unit 109A, and a power supply unit 110A.

The portable telephone 100A is specifically a computer system comprised of a microprocessor, a ROM, a RAM, a display unit, and the like. The ROM stores thereon a computer program. The portable telephone 100A pursues its function by the microprocessor performing according to the computer program.

The portable telephone 200A has the same structure as the portable telephone 100A, therefore the description thereof is omitted.

(1) The output unit 101A

The output unit 101A receives, from the recording medium 300A, list information having at least one piece of communication information that the user owns, displays a list of the communication information that the user owns, with use of the received list information, and prompts the user to input number-to-be used information that indicates the communication information that the user wants to use.

Further, if the output unit 101A receives, from the recording medium 300A, combination-impossible information indicating that there is no process information corresponding to both of the number-to-be used information and the authentication information, the output unit 101A outputs a message reporting that there is no process information corresponding to both of the number-to-be used information and

the user information.

The output unit 101A also outputs the same kinds of messages as the output unit 101 of the first embodiment.

(2) The fingerprint input unit 107A

The fingerprint input unit 107A is the same as the fingerprint input unit 107 of the first embodiment, therefore the description thereof is omitted here.

(3) The input unit 102A

The input unit 102A is comprised of a touch panel, a keyboard having ten key input function, and the like, and outputs to the control unit 108A an input instruction from the user, the input instruction including coordinates information showing the location at the touch panel that has been pushed, and a key operation signal generated by a key input through the keyboard.

When the list of communication information is displayed by the output unit 101A, the input unit 102A accepts number-to-be used information showing the communication information that the user wants to use, and outputs the accepted number-to-be used information to the control unit 108A.

The input unit 102A also accepts input of the same kinds of information as the input unit 102 of the first embodiment, and outputs these pieces of accepted information to the control unit 108A.

(4) The radio unit 103A

The radio unit 103A is the same as the radio unit 103 of the first embodiment, therefore the description thereof is omitted.

(5) The baseband signal process unit 104A

The baseband signal process unit 104A is the same as the baseband signal process unit 104 of the first embodiment, therefore the description thereof is omitted.

(6) The speaker 105A

The speaker 105A is the same as the speaker 105 of the first embodiment, therefore the description thereof is omitted.

(7) The microphone 106A

The microphone 106A is the same as the microphone 106 of the first embodiment, therefore the description thereof is omitted.

(8) The control unit 108A

The control unit 108A controls the portable telephone 100A as a whole.

The control unit 108A, upon receiving the list information from the recording medium 300A, outputs the received list information to the output unit 101A. The control unit 108A also receives number-to-be used information from the input unit 102A, and outputs the received number-to-be used information to the recording medium 300A.

The control unit 108A also receives, from the recording medium 300A, the same kinds of information as the control unit

108 of the first embodiment, and outputs these pieces of received information to the output unit 101A. Furthermore, the control unit 108A receives, from the input unit 102A, the same kinds of information as the control unit 108 of the first embodiment, and outputs these pieces of received information to the recording medium 300A.

Further, the control unit 108A, upon receiving combination-impossible information from the recording medium 300A, outputs the received combination-impossible information to the output unit 101A.

In addition, the control unit 108A owns a memory just as the control unit 108 of the first embodiment does.

(9) The input/output unit 109A

The input/output unit 109A is the same as the input/output unit 109 of the first embodiment, therefore the description thereof is omitted.

(10) The power supply unit 110A

The power supply unit 110A is the same as the power supply unit 110 of the first embodiment, therefore the description thereof is omitted.

2.3 The structure of the recording medium 300A

In this section, the structure of the recording medium 300A is described.

As shown in FIG. 11, the recording medium 300A is comprised of a storage area 310A, a control unit 320A, a setting unit

330A, and an input/output unit 340A.

The recording medium 300A is specifically a computer system which is comprised of a microprocessor, a ROM, a RAM, and the like. The ROM stores thereon a computer program. The recording medium 300A pursues its function by the microprocessor performing according to the computer program.

(1) The storage area 310A

The storage area 310A includes a first storage area 311A, a second storage area 312A, a third storage area 313A, and a process-name storage area 315A. The storage area 310A further includes a memory A 361A, a memory B 362A, a game 363A, a communication function 364A, and an electronic commerce function 365A, that are respectively either data or a function accessible to a user. Note here that the memory A 361A, the memory B 362A, the game 363A, the communication function 364A, and the electronic commerce function 365A have been prestored in the recording medium 300A before purchase.

(a) The first storage area 311A

The first storage area 311A has an authentication information table T350, one example of which is shown in FIG. 12.

This authentication information table T350 stores thereon at least one set of authentication number and authentication information.

Each set of items therein is the same as that in the

authentication information table T300 of the first embodiment, therefore further description is omitted here.

(b) The third storage area 313A

The third storage area 313A has a communication information table T351, one example of which is shown in FIG. 13.

The communication information table T351 stores thereon at least one set of communication number and communication information. The communication number is a number assigned to each piece of communication information. The communication information is a telephone number used when the portable telephone 100A is used as a telephone.

(c) The second storage area 312A

The second storage area 312A has a process information table T352, one example of which is shown in FIG. 14.

The process information table T352 stores thereon at least one set of process number and process information.

The process number is composed of first number and second number. A set of first number and second number uniquely identifies a piece of process information. Each first number represents a communication number, and each second number represents an authentication number.

The process information shows a name of a process which becomes accessible after authentication.

The process which becomes accessible after authentication

includes a memory function, a communication function, an electronic commerce function, and a game function, all of which require access to the data stored in the memory of the recording medium 300A. The process information is a name of process that corresponds to one of these functions.

Here, the process information representing a memory function is "memory A" and "memory B", which represent the names for the memory A 361A and the memory B 362A, each memory being a memory area that the storage area 310A owns. Likewise, the process information representing a game function is "game" which represents the name of the game 363A.

If "memory A" has been registered as process information, such processes are enabled as writing to and reading from the data files within the area of the memory A 361A, and registering of a new data file to the area of the memory A 361A. The same thing as the aforementioned case of "memory A" applies to the case in which "memory B" has been registered. The stated arrangement enables to use a proper memory area in storing information acquired through such as the communication function according to importance level of the information, and then to set communication number and authentication number to each memory area.

If "game" has been registered, it enables use of program data and data files necessary for the execution of the game 363A. The game is executed by using these program data and

data files.

If "communication function" has been registered, it enables use of program data and data files necessary for the execution of the communication function 364A. The communication function is executed by using these program data and data files.

If "electronic commerce function" has been registered, it enables use of program data and data files necessary for the execution of the electronic commerce function 365A. The electronic commerce function is executed by using these program data and data files.

Note here that the same authentication information may be assigned to different pieces of communication information. In the process information table T352, for example, an authentication number "3" is assigned to two different communication numbers 1 and 3. The process information assigned to the set of communication number "1" and authentication number "3" is "memory B"; and the process information assigned to the set of communication number "3" and authentication number "3" is "game".

(d) The process-name storage area 315A

The process-name storage area 315A is the same as the process-name storage area 315 of the first embodiment, therefore the description thereof is omitted.

(2) The setting unit 330A

The setting unit 330A is tamper-resistant, and includes therein an authentication-information setting unit 331A, a process-information setting unit 332A, and a communication-information setting unit 333A.

(a) The authentication-information setting unit 331A

As described as follows, the authentication-information setting unit 331A registers authentication information received from an external terminal into the first storage area 311A, either at the time when the recording medium 300A is purchased or at the time when it is commenced to be used.

The authentication-information setting unit 331A receives, as authentication information, one of character information, fingerprint information, and a combination of character information and fingerprint information from the external terminal via the input/output unit 340A, then judges whether the received authentication information has been already registered. If the authentication information has been already registered, the authentication-information setting unit 331A acquires the corresponding authentication number, and stores the acquired authentication number temporarily in the setting unit 330A.

Note here that the method of judging whether the received authentication information has been registered is the same as that of the first embodiment, therefore the description thereof is omitted here.

If the authentication information has not been registered yet, the authentication-information setting unit 331A registers the authentication information. The registration of the authentication information performed by the authentication-information setting unit 331A is the same as that performed by the authentication-information setting unit 331, therefore the description thereof is omitted here.

(b) The communication-information setting unit 333A

As described as follows, the communication-information setting unit 333A registers communication information received through an external terminal into the third storage area 313A, either at the time when the recording medium 300A is purchased or at the time when it is commenced to be used.

The communication-information setting unit 333A receives a telephone number from the input/output unit 340A via the control unit 320A, judges whether the received telephone number has been already registered. If the telephone number has been already registered, the communication-information setting unit 333A acquires the corresponding communication number, and stores the acquired communication number temporarily in the setting unit 330A.

If not yet been registered, the telephone number will be registered as follows. The communication-information setting unit 333A calculates, with use of the communication Information table T351, a communication number to be used for

the telephone number, and registers the telephone number with the calculated communication number into the communication-information table T351 of the third storage area 313A. Note here that the calculated communication number will be temporarily stored in the setting unit 330A.

(c) The process-information setting unit 332A

As described as follows, the process-information setting unit 332A registers process information received from an external terminal into the second storage area 312A, either at the time when the recording medium 300A is purchased or at the time when it is commenced to be used.

The process-information setting unit 332A receives process information to be registered into the second storage area 312A, from the input/output unit 340A via the control unit 320A. The process-information setting unit 332A then registers into the process information table T352 the received process information together with the communication number and the authentication number that have been temporarily stored in the setting unit 330A. The process-information setting unit 332A further makes inaccessible the process for the process name registered as the process information.

Note, in the above, that if process information that has the same communication number and the same authentication number has been already registered, another registration therefor will not be performed.

By the above operations, each set of communication information and authentication information is associated with the corresponding process information.

(3) The control unit 320A

The control unit 320A is tamper-resistant, and includes an authentication unit 321A, a process unit 322A, and a selection unit 323A.

The control unit 320A receives authentication-start information and other kinds of information, from the portable telephone 100A via the input/output unit 340A. Upon receiving information from the portable telephone 100A, the control unit 320A judges whether the received information is authentication-start information or not. If judging that it is authentication-start information, the control unit 320A outputs the received authentication-start information to the authentication unit 321A, and makes the authentication unit 321A start authentication. If the received information is judged not to be authentication-start information, authentication will not be performed.

(a) The selection unit 323A

The selection unit 323A, upon receiving an instruction to output list information from the authentication unit 321A, generates list information composed of the telephone numbers stored in the communication information table T351 of the third storage area 313A, then outputs the generated list information

to the portable telephone 100A via the input/output unit 340A, in order to prompt the user to select communication information that he wants to use.

The selection unit 323A receives number-to-be used information from the portable telephone 100A via the input/output unit 340A, and acquires the communication number that corresponds to the received number-to-be used information. In addition, the selection unit 323A retains the acquired communication number and the corresponding communication information until the next authentication.

(b) The authentication unit 321A

The authentication unit 321A, upon receiving authentication-start information from the control unit 320A, instructs the selection unit 323A to output list information.

After the communication number has been acquired at the selection unit 323A, the authentication unit 321A outputs the input-means information to the portable telephone 100A via the input/output unit 340A.

The authentication unit 321A receives from the portable telephone 100A one of first input information, second input information, and third input information. Then according to the received input information, the authentication unit 321A receives user information from the portable telephone 100A, just as shown in the first embodiment. The authentication unit 321A then performs authentication with use of the received user

information and the authentication information table T350, and in case when it is necessary to output an acquired authentication number to the process unit 322A, outputs the acquired authentication number and the communication number acquired at the selection unit 323A, as a set, to the process unit 322A.

Note here that the authentication method is the same as that performed by the authentication unit 321 of the first embodiment, therefore the description thereof is omitted here.

(c) The process unit 322A

The process unit 322A receives an authentication number and a communication number from the authentication unit 321A, and judges whether there is a set of first number and second number that matches the received set of authentication number and communication number.

If such set of first number and second number exists, the following operation will be performed. First, the process unit 322A judges whether process-in-use information is stored in the process-name storage area 315A. If the process-in-use information is stored, the process unit 322A reads it from the process-name storage area 315A, and acquires the process name of the process that has been made accessible. Then the process unit 322A sets access right so that the process for the acquired process name is made inaccessible. Next, the process unit 322A reads, from the process information table T352, the process information that corresponds to the set of first number and

second number that matches the received set of authentication number and communication number, and sets access right so that only the process of the process name registered in the read process information is accessible. Further, the process unit 322A updates the content of the process-name storage area 315A, so that the process name registered in the acquired process information will be new process-in-use information.

If no such set of first number and second number exists, the process unit 322A generates combination-impossible information, and outputs the generated combination-impossible information to the portable telephone 100A via the input/output unit 340A.

After authentication, the process unit 322A receives information indicating process execution from the portable telephone 100A via the input/output unit 340A, and performs, using the received information, various controls targeted to such as a communication function, an electronic commerce function, and a memory function. If the communication function is used, the process unit 322A communicates with the base station using the communication information selected in the selection unit 323A. Note that in transmitting information to the base station, the process unit 322A encodes the information in advance, just as conventional portable telephones do. The reception of information from the base station is also performed in the same way as in conventional telephones.

(4) The input/output unit 340A

The input/output unit 340A is the same as the input/output unit 340 of the first embodiment, therefore the description thereof is omitted.

2.4 The operations of the recording-medium unauthorized use prevention system 2

In this section, each operation of the recording-medium unauthorized use prevention system 2 is described.

(1) The setting operations for communication information, authentication information, and process information

Here, the operations for setting communication information, authentication information, and process information are described with reference to the flowchart of FIG. 15.

The communication-information setting unit 333A receives, from the input/output unit 340A, communication information inputted through an external device (Step S100), and judges whether the received communication information has been already registered (Step S105). If the received communication information has not been registered yet, the communication-information setting unit 333A calculates a communication number with use of the communication information table T351, registers the calculated communication number together with the received communication information into the communication information table T351 of the third storage area

313A, and temporarily stores therein the calculated communication number for the process-information setting unit 332A to be able to refer to (Step S115). Next, the authentication-information setting unit 331A receives, from the input/output unit 340A, authentication information inputted through the external device (Step S120), and judges whether the received authentication information has been already registered (Step S125). If the received authentication information has not yet been registered, the authentication-information setting unit 331A calculates an authentication number with use of the authentication information table T350, registers the calculated authentication number together with the received authentication information into the authentication information table T350 of the first storage area 311A, and temporarily stores therein the calculated authentication number for the process-information setting unit 332A to be able to refer to (Step S135). The process-information setting unit 332A receives process information (Step S140), then sets the temporarily stored communication number as a first number and the temporarily stored authentication number as a second number, and judges whether the first number and the second number, as a set, have been in use or not (Step S145). If this set of first number and second number is not in use, the process-information setting unit 332A registers the first number, the second number, and the received process information

into the process information table T352, and sets the process corresponding to the process name of the registered process information inaccessible (Step S150). If this set of first number and second number is in use, the operation ends there.

Note here that the process information registered at Step S150 may be either process information not yet registered in the process-information table T352, or may be already registered process information.

If the received authentication information has been already registered, the authentication-information setting unit 331A acquires the corresponding authentication number, and temporarily stores therein the acquired authentication number for the process-information setting unit 332A to be able to refer to (Step S130), and the operation from Step S140 will be performed.

If the received communication information has been already registered, the communication-information setting unit 333A acquires the corresponding communication number, and temporarily stores therein the acquired communication number for the process-information setting unit 332A to be able to refer to (Step S110), and the operation from Step S120 will be performed.

If only communication information should be registered, the received communication information is judged at Step S105 whether it has already been registered, and if the communication

information has been registered, the operation ends there. If the communication information has not been registered, Step S115 will be performed, then the operation ends.

If only authentication information should be registered, Step S120 is performed. Then at Step S125, the received authentication information is judged whether it has already been registered, and if the authentication information has been registered, the operation ends there. If the authentication information has not been registered, Step S135 will be performed, then the operation ends.

Further, if only process information should be registered, it will be realized by receiving already registered process information, at Step S100, and receiving already registered authentication information, at step S120.

(2) The authentication operation

Here, the authentication operation is described with reference to the flowchart of FIG. 16.

The control unit 320A receives information from the portable telephone 100A (Step S195), and judges whether the received information is authentication-start information or not (Step S198). If it is judged not to be authentication-start information, authentication will not be performed. If it is judged to be authentication-start information, the control unit 320A outputs the authentication-start information to the authentication unit 321A (Step S200). Upon receiving the

authentication-start information, the authentication unit 321A instructs the selection unit 323A to output list information (Step S201).

The selection unit 323A generates the list information with use of each telephone number registered in the communication information table T351, and outputs the generated list information to the portable telephone 100A (Step S203). Next, the selection unit 323A receives number-to-be used information from the portable telephone 100A via the input/output unit 340A, and acquires a communication number for the communication information that corresponds to the received number-to-be used information (Step S205). Note here that until the number-to-be used information is received, the operation is in a state of waiting to receive such number-to-be used information at Step S205.

Next, the authentication unit 321A generates input-means information, and outputs the generated input-means information to the portable telephone 100A (Step S206). The authentication unit 321A receives, from the portable telephone 100A, one of first input information, second input information, and third input information (Step S207), and performs operation for accepting user information (Step S210).

Next, the authentication unit 321A judges whether the authentication information table T350 has authentication information that matches the received user information (Step

S215).

If there is authentication information matching the received user information, the authentication unit 321A acquires the authentication number of the matching authentication information from the authentication information table T350, and outputs the acquired authentication number and the communication number acquired at Step S205 to the process unit 322A (Step S220). The process unit 322A judges whether there is process information that corresponds to the acquired set of communication number and authentication number (Step S240). If there is such process information, the access right setting operation is performed (Step S245).

If there is no process information that corresponds to the set of communication number and authentication number, the process unit 322A generates combination-impossible information, and outputs the generated combination-impossible information to the portable telephone 100A via the input/output unit 340A (Step S250).

If there is no authentication information that matches the received user information, the authentication unit 321A generates authentication-impossible information, and outputs the generated authentication-impossible information to the portable telephone 100A via the input/output unit 340A (Step S225). Next, the authentication unit 321A judges, from the authentication information table T350, whether there is any

authentication-unnecessary number (Step S230). If there is such authentication-unnecessary number, the authentication unit 321A acquires the authentication-unnecessary number (Step S235), and performs the operation from Step S240. If there is no authentication-unnecessary number, the operation ends there.

(3) The user information reception operation

The user information reception operation shown in FIG. 16 is the same as the user information reception operation of the first embodiment which is shown in FIG. 8. Therefore, the description is omitted here.

(4) The access right setting operation

Here, the access right setting operation mentioned in FIG. 16 is detailed with reference to the flowchart of FIG. 17.

The process unit 322A judges whether there is process-in-use information (Step S260).

If there is process-in-use information, the process unit 322A reads the process-in-use information from the process-name storage area 315A, acquires the process name of the process that has been made accessible, and sets access right so that the process corresponding to the acquired process name is made inaccessible (Step S265). The process unit 322A then acquires process information that corresponds to the set of first number and second number, which matches the set of communication number

and authentication number that has been received from the authentication unit 321A. The process unit 322A sets access right to the process for the process name registered in the acquired process information, so that the process is made accessible (Step S270). The process unit 322A updates the process-in-use information of the process-name storage area 315A, using the process name registered in the process information acquired at Step S270.

If there is no process-in-use information, the operation from Step S270 will be performed.

(5) Examples of authentication operation

Here, a specific flow of the authentication operation is described with reference to each table shown in FIGs. 12, 13, and 14.

The selection unit 323A, upon receiving from the portable telephone 100A communication information of "corporate", acquires the communication number of "1".

The authentication unit 321A, upon receiving from the portable telephone 100A, fingerprint information as user information, acquires the authentication number of "2" from the authentication information table T350.

The process unit 322A acquires the first number "1" and the second number "2", from the communication number "1" and the authentication number "2", and acquires the process information that corresponds to both of the acquired first number

"1" and the second number "2" from the process information table T352. In this case, the process information in which "communication function" has been registered is acquired, and the communication function will be made accessible.

If the selection unit 323A receives communication information of "corporate", and the authentication unit 321A receives character information of "PW2" as user information, the communication function and the electronic commerce function are made accessible.

If the selection unit 323A receives communication information of "corporate", and the authentication unit 321A receives character information of "PW10" as user information, a message reporting that there is no authentication information that matches the "PW10" in the authentication information table T350 is outputted to the portable telephone 100A.

Further, the authentication unit 321A judges whether there is any authentication-unnecessary number in the authentication information table T350, and acquires the authentication number "1". The process unit 322A acquires the first number "1" and the second number "1" from the communication number "1" and the authentication number "1", and acquires the process information that corresponds to both of the acquired first number "1" and the second number "1", from the process information table T352. In this case, the process information in which "memory B" has been registered is acquired, then this memory

B is made accessible.

If the selection unit 323A receives communication information of "private 1", and the authentication unit 321A receives character information of "PW2", the process unit 322A acquires the first number "2" and the second number "3", from the communication number "2" and the authentication number "3", and judges whether the process information table T352 has process information that matches both of the acquired first number "2" and the second number "3". In this case, there is no process information that matches both of the first number "2" and the second number "3", therefore a message reporting that there is no such process information is outputted to the portable telephone 100A.

2.5 Summary of the second embodiment

As described above, the recording-medium unauthorized use prevention system 2 has, within the recording medium 300A, an authentication unit 321A that is tamper-resistant. This prevents third parties from decoding and tampering the authentication structure of the authentication unit. Therefore, it prevents unauthorized third parties from accessing the recording medium 300A.

In addition, the recording medium 300A stores thereon one or more pieces of communication information, one or more pieces of authentication information, and further one or more pieces of process information that each correspond to a piece

of communication information and to a piece of authentication information. Therefore, the user can use appropriate communication information and user information according to functions he wants to use. This makes it possible to restrict use of functions stored in the recording medium 300A, thereby heightening security. Therefore, the recording medium 300A will have heightened security for the owner.

In addition, while conventional recording media record thereon only one communication information, the recording medium 300A stores thereon a plurality of pieces of communication information. Therefore, the user of the recording medium 300A does not have to carry a plurality of recording media, which reduces possibility of unauthorized use thereof, incident to loss or robbery.

For example, there is a system that a user ID card which is called an SIM (subscriber identity module) card is mounted to the main body of a telephone so as to enable communication. This SIM card stores therein individual information of the owner, such as an ID code and telephone number data. By mounting this SIM card to such as a portable telephone of the user, a telephone of others, and a public telephone, it becomes possible to perform various operations with use of the ID code stored in the SIM card, such as calling and billing, and even calling based on the telephone number data stored in the memory is made possible.

However, One SIM card can store therein only one ID code

and related information. Therefore, if a person owns a plurality of ID codes, he accordingly has to own the corresponding number of SIM cards. However, the recording medium of the second embodiment is operable to store therein a plurality of pieces of communication information. Therefore, even if a person owns a plurality of ID codes, he has to carry only one recording medium. This reduces possibility of unauthorized use incident to loss or robbery.

3. The third embodiment

As the third embodiment according to the present invention, a recording-medium unauthorized use prevention system 3 is described as follows.

3.1 The structure of a recording-medium unauthorized use prevention system 3

The recording-medium unauthorized use prevention system 3 has the same structure as the recording-medium unauthorized use prevention systems 1 and 2, and is comprised of portable telephones 100B, 200B, and a recording medium 300B to which each portable telephone is mountable.

In this section, the description mainly focuses on the differences with the recording-medium unauthorized use prevention systems 1 and 2.

The recording-medium unauthorized use prevention system 3 detects the incident when the recording medium 300B is mounted

to the portable telephone 100B, records information indicating thereof, into the recording medium 300B, and judges whether it is necessary to receive a password by comparing the information recorded this time with the information recorded last time, the password being composed of a combination of such as one or more numbers and alphabets, and being used for identifying the owner of the recording medium 300B. Hereinafter, the password is called "input password."

When reception of an input password is necessary, the recording-medium unauthorized use prevention system 3 receives the input password, and if the input password matches the password prestored in the recording medium 300B receives communication information and user information, so as to enable restriction of accessible process information, just as in the second embodiment.

Note here that the same operation as in the above will be performed when the power is turned on while the recording medium 300B is being mounted to the portable telephone 100B.

The same thing applies to the case when the recording medium 300B is mounted to the portable telephone 200B.

3.2 The structure of the portable telephone 100B

In this section, the description focuses on the difference with the portable telephone 100 or with the portable telephone 100A.

As shown in FIG. 18, the portable telephone 100B is

comprised of an output unit 101B, an input unit 102B, a radio unit 103B, a baseband signal process unit 104B, a speaker 105B, a microphone 106B, a fingerprint input unit 107B, a control unit 108B, an input/output unit 109B, a power supply unit 110B, and a connection unit 115B.

The portable telephone 100B is specifically a computer system comprised of a microprocessor, a ROM, a RAM, a display unit, and the like. The ROM stores thereon a computer program. The portable telephone 100B pursues its function by the microprocessor performing according to the computer program.

Note here that the portable telephone 200B has the same structure as the portable telephone 100B, therefore the description thereof is omitted.

(1) The output unit 101B

The output unit 101B receives, from the recording medium 300B, a password input request indicating an input request of an input password, outputs a message prompting the user to input an input password.

Further, if the output unit 101B receives identification-impossible information indicating that the input password inputted through the input unit 102B does not match the password stored in the recording medium 300B, outputs a message reporting thereof.

Furthermore, the output unit 101B outputs the same messages as those outputted from the output unit 101 of the

first embodiment, or as those outputted from the output unit 101A of the second embodiment.

(2) The fingerprint input unit 107B

The fingerprint input unit 107B is the same as the fingerprint input unit 107 of the first embodiment, therefore the description thereof is omitted here.

(3) The input unit 102B

The input unit 102B is comprised of a touch panel, a keyboard having ten key input function, and the like, and outputs to the control unit 108B an input instruction from the user, the input instruction including coordinates information showing the location at the touch panel that has been pushed, and a key operation signal generated by a key input through the keyboard.

In addition, when the output unit 101B outputs a message prompting the user to input of an input password, the input unit 102B receives the input password, and outputs the received input password to the control unit 108B.

The input unit 102B also accepts input of the same kinds of information as those accepted by the input unit 102 of the first embodiment or by the input unit 102A of the second embodiment, and outputs these pieces of accepted information to the control unit 108B.

(4) The radio unit 103B

The radio unit 103B is the same as the radio unit 103

of the first embodiment, therefore the description thereof is omitted.

(5) The baseband signal process unit 104B

The baseband signal process unit 104B is the same as the baseband signal process unit 104 of the first embodiment, therefore the description thereof is omitted.

(6) The speaker 105B

The speaker 105B is the same as the speaker 105 of the first embodiment, therefore the description thereof is omitted.

(7) The microphone 106B

The microphone 106B is the same as the microphone 106 of the first embodiment, therefore the description thereof is omitted.

(8) The control unit 108B

The control unit 108B controls the portable telephone 100B as a whole.

The control unit 108B, upon receiving a password input request from the recording medium 300B via the input/output unit 109B, outputs the received password input request to the output unit 101B.

The control unit 108B receives from the input unit 102B either number-to-be used information or an input password, outputs the number-to-be used information or the input password to the recording medium 300B.

The control unit 108B, upon receiving an

identification-impossible information from the recording medium 300B via the input/output unit 109B, outputs the received identification-impossible information to the output unit 101B.

The control unit 108B also receives, from the recording medium 300B, the same kinds of information as the control unit 108 of the first embodiment, and as the control unit 108A of the second embodiment, and outputs these pieces of received information to the output unit 101B. Further, the control unit 108B receives, from the input unit 102B, the same kinds of information as the control unit 108 of the first embodiment, or as the control unit 108A of the second embodiment, and outputs there pieces of received information to the recording medium 300B.

In addition, the control unit 108B has a calendar function and a clock function, and upon receiving information for inquiring about the current date and time from the recording medium 300B, acquires the current date and time with use of the calendar function and the clock function, and outputs the acquired date and time to the recording medium 300B.

Furthermore, the control unit 108B has a GPS(global positioning system) function, and upon receiving information for inquiring about the current position from the recording medium 300B, acquires the current position information by communicating with the GPS satellites via the radio unit 103B, and outputs the acquired current position information to the recording medium

300B.

Here, the date and time to be outputted to the recording medium 300B is date, hour, and minute, and the position information to be outputted to the recording medium 300B is in a unit of municipalities.

In addition, the control unit 108B owns a memory just as the control unit 108 of the first embodiment does.

(9) The input/output unit 109B

The input/output unit 109B is the same as the input/output unit 109 of the first embodiment, therefore the description thereof is omitted.

(10) The power supply unit 110B

The power supply unit 110B is the same as the power supply unit 110 of the first embodiment, therefore the description thereof is omitted.

(11) The connection unit 115B

The connection unit 115B has therein a pullup resistor 130B and a ground 131B, as shown in FIG. 19.

One end of the pullup resistor 130B is connected to the power supply unit 110B, and the other end thereof is connected to a detection unit of the recording medium 300B, which will be detailed later. In addition, the ground 131B is connected to the power supply unit 110B and to the detection unit of the recording medium 300B.

By the above arrangement, when the recording medium 300B

is mounted to the portable telephone 100B, the portable telephone 100B is able to send, with use of the power voltage of the power supply unit 110B, to the detection unit of the recording medium 300B, a mounting-detect signal indicating that the recording medium 300B has been mounted to the portable telephone 100B. While the recording medium 300B is being mounted, the portable telephone 100B continues outputting the mounting-detect signal to the detection unit of the recording medium 300B.

3.3 The structure of the recording medium 300B

In this section, the structure of the recording medium 300B is described.

As shown in FIG. 20, the recording medium 300B is comprised of a storage area 310B, a control unit 320B, a setting unit 330B, an input/output unit 340B, and a judgment unit 350B.

The recording medium 300B is specifically a computer system which is comprised of a microprocessor, a ROM, a RAM, and the like. The ROM stores thereon a computer program. The recording medium 300B pursues its function by the microprocessor performing according to the computer program.

(1) The storage area 310B

The storage area 310B includes a first storage area 311B, a second storage area 312B, a third storage area 313B, a password storage area 314B, and a process-name storage area 315B. The storage area 310B further includes a memory A 361B, a memory B 362B, a game 363B, a communication function 364B, and an

electronic commerce function 365B, just as the storage area 310A of the second embodiment. Note here that the memory A 361B, the memory B 362B, the game 363B, the communication function 364B, and the electronic commerce function 365B have been prestored in the recording medium 300B before purchase.

(a) The first storage area 311B

The first storage area 311B is the same as the first storage area 311A of the second embodiment, therefore the description thereof is omitted here.

(b) The second storage area 312B

The second storage area 312B is the same as the second storage area 312A of the second embodiment, therefore the description thereof is omitted here.

(c) The third storage area 313B

The third storage area 313B is the same as the third storage area 313A of the second embodiment, therefore the description thereof is omitted here.

(d) The password storage area 314B

The password storage area 314B stores thereon the password that identifies the owner of the recording medium 300B, that is used in judging whether a user matches the owner of the recording medium 300B.

Note that hereinafter, the password stored in the password storage area 314B is called "registration password."

(e) The process-name storage area 315B

The process-name storage area 315B is the same as the process-name storage area 315 of the first embodiment, and as the process-name storage area 315A of the second embodiment, therefore the description thereof is omitted here.

(2) The judgment unit 350B

The judgment unit 350B includes therein a detection unit 351B, a controller 352B, and a history information recording unit 353B.

(a) The detection unit 351B

When the recording medium 300B is mounted to the portable telephone 100B, the detection unit 351B is connected to the connection unit 115B that is included in the portable telephone 100B, receives a mounting-detect signal from the connection unit 115B, and outputs the received mounting-detect signal to the history information recording unit 353B via the controller 352B.

While the recording medium 300B is being mounted to the portable telephone 100B, the detection unit 351B continues outputting the mounting-detect signal to the history information recording unit 353B via the controller 352B.

(b) The controller 352B

The controller 352B receives the mounting-detect signal from the detection unit 351B, and outputs the received mounting-detect signal to the history information recording unit 353B. The controller 352B also outputs information

received from the history information recording unit 353B to the input/output unit 340B; and further performs input/output of information with the portable telephone 100B via the input/output unit 109B of the portable telephone 100B.

(c) The history information recording unit 353B

The history information recording unit 353B has a history information storage area 354B for storing therein history information. The history information storage area 354B includes a history information table T400, one example of which is shown in FIG. 21. Here, the history information is composed of: category information showing that the recording medium 300B is mounted to the portable telephone 100B; date/time information showing the date and time in which the recording medium 300B is mounted to the portable telephone 100B; and position information showing the position at which the recording medium 300B is mounted to the portable telephone 100B.

The history information table T400 stores therein at least one set of such history information showing category, date/time, and position.

"Category" in this figure represents category information indicating that the recording medium 300B is mounted to the portable telephone 100B; "date/time" in this figure represents date/time information indicating the date and time of the mounting; and "position" therein represents position information indicating the position of the mounting and is

registered in a unit of municipalities.

When the recording medium 300B is mounted, the history information recording unit 353B receives a mounting-detect signal from the controller 352B. Upon receiving the mounting-detect signal, the history information recording unit 353B outputs to the portable telephone 100B information for inquiring about the current date/time and the current position, receives from the portable telephone 100B information on the current date/time and information on the current position, generates history information with use of each piece of the received information, and registers the generated history information into the history information table T400. After the registration of the history information, the history information recording unit 353B outputs authentication-instruction information for instructing authentication-start, to the authentication unit 321B.

(3) The setting unit 330B

The setting unit 330B is tamper-resistant, and includes therein an authentication-information setting unit 331B, a process-information setting unit 332B, and a communication-information setting unit 333B.

(a) The authentication-information setting unit 331B

The authentication-information setting unit 331B registers authentication information into the first storage area 311B, and a registration password into the password storage

area 314B.

The registration of the registration password is performed as follows. That is, the authentication-information setting unit 331B receives, from the input/output unit 340B via the control unit 320B information composed of the registration password and information for instructing registration of the registration password, and registers the registration password into the password storage area 314B with use of the received information. Note that the registration password can be changed even after registration.

The registration of authentication information is the same as those of the first embodiment and the second embodiment, therefore the description thereof is omitted.

Note that the setting of the registration password is performed from an external terminal or from the portable telephone 100B, and the registration of the authentication information is performed from an external terminal.

(b) The communication-information setting unit 333B

The communication-information setting unit 333B receives communication information from the input/output unit 340B via the control unit 320B, and registers the received communication information.

The registration of the communication information is the same as that performed by the communication-information setting unit 333A shown in the second embodiment, therefore the

description thereof is omitted here.

(c) The process-information setting unit 332B

The process-information setting unit 332B receives process information from the input/output unit 340B via the control unit 320B, and registers the process information.

The registration of the process information is the same as that performed by the process-information setting unit 332A shown in the second embodiment, therefore the description thereof is omitted here.

(4) The control unit 320B

The control unit 320B is tamper-resistant, and includes an authentication unit 321B, a process unit 322B, and a selection unit 323B.

The control unit 320B receives authentication-start information and other kinds of information, from the portable telephone 100B via the input/output unit 340B. Upon receiving information from the portable telephone 100B, the control unit 320B judges whether the received information is authentication-start information or not. If judging that it is authentication-start information, the control unit 320B outputs the received authentication-start information to the authentication unit 321B, and makes the authentication unit 321B start authentication. If the received information is judged not to be authentication-start information, authentication will not be performed.

(a) The authentication unit 321B

Here, the authentication unit 321B is described.

(i) The authentication while the recording medium 300B is being mounted

The authentication unit 321B, upon receiving authentication-instruction information from the history information recording unit 353B, reads first history information that is the latest history information and second history information that is the history information last time, then calculates the difference in date/time therebetween, with use of the date/time item of the first history information and the date/time item of the second history information. Then, the authentication unit 321B judges whether the calculated difference in date/time exceeds the predetermined time interval prestored in the authentication unit 321B. In this example, the predetermined time interval prestored in the authentication unit 321B is 30 minutes, and is set at the time of purchase of the recording medium 300B from an external terminal.

If the difference in date/time is judged to exceed the predetermined time interval, the authentication unit 321B outputs a password input request to the portable telephone 100B via the input/output unit 340B.

If the difference in date/time is judged not to exceed the predetermined time interval, the authentication unit 321B judges whether the position of mounting differs between the

first history information and the second history information. If the positions of mounting are judged to be identical, the authentication unit 321B outputs to the process unit 322B authentication-unnecessary information for instructing not to perform authentication. On the contrary, if the positions of mounting are judged to differ, the authentication unit 321B outputs a password input request to the portable telephone 100B via the input/output unit 340B.

When receiving the input password from the portable telephone 100B, the authentication unit 321B judges whether the received input password matches the registration password stored in the password storage area 314B. If it is judged to match, the authentication unit 321B instructs the selection unit 323B to output list information.

If it is judged not to match, the authentication unit 321B outputs a message reporting that the input password is not correct, to the portable telephone 100B via the input/output unit 340B.

Note that the operation from instructing to the selection unit 323B to output list information is the same as that performed by the authentication unit 321A of the second embodiment, therefore the description thereof is omitted.

(ii) The authentication according to a user instruction

The authentication unit 321B receives

authentication-start information from the control unit 320B. Upon receiving the authentication-start information, the authentication unit 321B outputs a password input request to the portable telephone 100B via the input/output unit 340B. Upon receiving an input password from the portable telephone 100B, the authentication unit 321B judges whether the received input password matches the registration password that has been registered in the password storage area 314B. If they are judged to match each other, the authentication unit 321B instructs the selection unit 323B to output list information.

If the passwords are judged not to match each other, the authentication unit 321B outputs to the portable telephone 100B via the input/output unit 340B, a message reporting that the input password is not correct.

Note that the operation from instructing the selection unit 323B to output list information is the same as that performed by the authentication unit 321A of the second embodiment, therefore the description thereof is omitted here.

(b) The process unit 322B

Here, the process unit 322B is described.

The process unit 322B receives either authentication-unnecessary information from the authentication unit 321B, or an authentication number and a communication number from the authentication unit 321B.

When receiving authentication-unnecessary information

from the authentication unit 321B, the process unit 322B judges whether process-in-use information has been stored in the process-name storage area 315B. If process-in-use information has been stored, it will be read from the process-name storage area 315B, and the process name is acquired from the read process-in-use information. Then, the access right is given to the process corresponding to the process whose process name has been acquired, so as to enable execution of the process.

When receiving an authentication number and a communication number from the authentication unit 321B, the process unit 322B performs the same operation as the process unit 322A of the second embodiment, therefore the description is omitted therefor.

(c) The selection unit 323B

The selection unit 323B, upon receiving from the authentication unit 321B information instructing to output list information, requests the portable telephone 100B to input number-to-be used information, and accepts the number-to-be used information corresponding to the number that the user wants to use.

Note that the acceptance of number-to-be used information is the same as that performed by the second embodiment, therefore the description is omitted here.

(5) The input/output unit 340B

The input/output unit 340B receives, from the controller

352B of the judgment unit 350B, information of either the portable telephone 100B or an external terminal, and outputs the received information either to the control unit 320B, or to the setting unit 330B via the control unit 320B, according to the content of the received information.

The input/output unit 340B also outputs information received from the control unit 320B, to the portable telephone 100B via the controller 352B of the judgment unit 350B.

3.4 The operations of the recording-medium unauthorized use prevention system 3

In this section, each operation of the recording-medium unauthorized use prevention system 3 is described. Note that the operations for setting authentication information, communication information, and process information are the same as those of the second embodiment, therefore the description thereof is omitted here.

(1) The registering operation of history information

Here, the operation for registering history information is described with reference to the flowchart shown in FIG. 22.

The detection unit 351B receives a mounting-detect signal from the connection unit 115B of the portable telephone 100B, by being connected to the connection unit 115B, and outputs the received mounting-detect signal to the controller 352B (Step S300).

The controller 352B, upon receiving the mounting-detect

signal, outputs the received mounting-detect signal to the history information recording unit 353B (Step S305).

The history information recording unit 353B, upon receiving the mounting-detect signal, outputs to the portable telephone 100B information inquiring about the current date/time and the current position, then receives from the portable telephone 100B information on the current date/time and information on the current position (Step S308). The history information recording unit 353B generates history information with use of each piece of the received information, and registers the generated history information into the history information table T400, and instructs the authentication unit 321B to start authentication (Step S310).

(2) The authentication operation

Here, the authentication operation is described with reference to the flowcharts shown in FIGs. 23 and 24.

Upon receiving an instruction to start authentication from the history information recording unit 353B, the authentication unit 321B acquires first history information and second history information from the history information table T400 (Step S400), and judges whether the difference between the date/time of mounting last time and the date/time of mounting this time is within a predetermined time period, with use of date/time items in the acquired pieces of information (Step S405).

If the difference is judged to be within the predetermined time period, the authentication unit 321B judges whether the position of mounting last time and the position of mounting this time differ from each other, with use of the position items in the acquired pieces of information (Step S410).

If the positions are judged to be the same, the authentication unit 321B outputs authentication-unnecessary information to the process unit 322B, and access right setting operation is performed at the process unit 322B (Step S475).

If the positions are judged to differ, the authentication unit 321B outputs a password input request to the portable telephone 100B, receives an input password from the portable telephone 100B (Step S415), and judges whether the received input password matches the registration password (Step S420).

If the mentioned passwords are judged not to match each other, the authentication unit 321B generates identification-impossible information, outputs the generated identification-impossible information to the portable telephone 100B, and ends the operation (Step S425).

If the mentioned passwords are judged to match each other, the selection unit 323B generates list information with use of each telephone number stored in the third storage area 313B, and outputs the generated list information to the portable telephone 100B (Step S430). Next, the number-to-be used information inputted from the portable telephone 100B is

received through the input/output unit 340B, and the communication number of the communication information that corresponds to the received number-to-be used information is acquired (Step S435). Note that until the number-to-be used information is received, the operation is in a wait state for receiving number-to-be used information, at Step S435.

Next, the authentication unit 321B generates input-means information, and outputs the generated input-means information to the portable telephone 100B (Step S436). The authentication unit 321B then receives, from the portable telephone 100B, one of first input information, second input information, and third input information (Step S437), and performs user information reception operation (Step S440).

Next, the authentication unit 321B judges whether there is, within the first storage area 311B, authentication information that matches the received user information (Step S445).

If there is such authentication information matching the received user information, the authentication unit 321B acquires the authentication number of this authentication information from the first storage area 311B, and outputs to the process unit 322B the acquired authentication number together with the communication number that has been acquired at Step S435 (Step S450). The process unit 322B judges whether there is process information that corresponds to the received

set of communication number and authentication number (Step S470). If there is such process information, access right setting operation is performed (Step S475). If there is no such process information that corresponds to the set of the communication number acquired at the selection unit 323B and the authentication number acquired at the authentication unit 321B, the process unit 322B generates combination-impossible information, and outputs the generated combination-impossible information to the portable telephone 100B via the input/output unit 340B (Step S480).

If there is no authentication information that matches the received user information, the authentication unit 321B generates authentication-impossible information, and outputs the generated authentication-impossible information to the portable telephone 100B via the input/output unit 340B (Step S455). Then judgment is performed whether any authentication-unnecessary number exists (Step S460). If no such authentication-unnecessary number exists, the operation ends there. If such an authentication-unnecessary number exists, it is acquired (Step S465), and the operation from Step S470 is performed.

If, at Step S405, the difference is judged not to be within the predetermined time period, the operation from Step S415 is performed.

Note that the authentication according to user instruction

is performed as follows.

That is, the control unit 320B receives information from the portable telephone 100B, and judges whether the received information is authentication-start information or not. If judging that it is authentication-start information, the control unit 320B outputs the received authentication-start information to the authentication unit 321B. After receipt of the authentication-start information, the operation from Step S415 shown in FIG. 23 is performed, so as to realize the authentication.

If the information received at the control unit 320B is judged not to be authentication-start information, authentication will not be performed.

(3) The user information reception operation

The user information reception operation shown in FIG. 23 is the same as the user information reception operation of the first embodiment which is shown in FIG. 8. Therefore, the description is omitted therefor.

(4) The access right setting operation

Here, the access right setting operation mentioned in FIG. 24 is detailed with reference to the flowchart of FIG. 25.

The process unit 322B judges whether authentication-unnecessary information is received from the authentication unit 321B (Step S500).

If authentication-unnecessary information is not received, the process unit 322B further judges whether there is process-in-use information (Step S505). If there is process-in-use information, the process unit 322B reads the process-in-use information and acquires the process name of the process having been made accessible, and sets access right so that the process corresponding to the acquired process name is made inaccessible (Step S510). Further, the process unit 322B acquires, from the second storage area 312B, process information corresponding to the set of first number and second number that matches the set of communication number and authentication number that has been received from the authentication unit 321B, sets access right to the process corresponding to the process name registered in the acquired process information, so that the process is made accessible (Step S515). The process unit 322B updates the process-in-use information in the process-name storage area 315B, with use of the process name registered in the process information acquired at Step S515 (Step S520). If there is no process-in-use information, the operation from Step S270 is performed.

If the process unit 322B judges that it has received authentication-unnecessary information, it further judges whether there is process-in-use information (Step S525). If there is process-in-use information, the process unit 322B reads process-in-use information from the process-name storage area

315B, acquires the process name of the process that has been made accessible, and sets access right to the process for the acquired process name, so that the process is made accessible (Step S530). If there is no process-in-use information, the operation ends there.

(5) Examples of authentication operation

Here, a specific flow of authentication operation up to Step S420 is described with use of the history information table T400 shown in FIG. 21. Note that the flow from Step S430 is the same as the corresponding authentication operation flow of the second embodiment, therefore the description is omitted here.

A case is taken as an example in which history information 402 has been registered as latest information.

The authentication unit 321B, upon receiving authentication-instruction information, acquires the history information 402 as first history information, and history information 401 as second history information. Then, the authentication unit 321B judges whether the latest mounting was performed within a predetermined time period, with use of date/time items in the acquired pieces of history information. Since the difference is 50 minutes in this case, the authentication unit 321B accepts an input password, and judges the correctness of the accepted input password.

Next, a case is detailed in which history information

403 has been registered as latest information.

The authentication unit 321B, upon receiving authentication-instruction information from the history information recording unit 353B via the input/output unit 340B, acquires the history information 403 as first history information, and the history information 402 as second history information. Then, the authentication unit 321B judges whether the latest mounting was performed within a predetermined time period, with use of date/time items in the acquired pieces of history information. Since the difference is 20 minutes in this case, the authentication unit 321B judges whether the mounting for the both times was performed at the same position. Since the positions of mounting are different in this case, therefore the authentication unit 321B accepts an input password, and judges the correctness of the accepted input password.

Next, a case is detailed in which history information 404 has been registered as latest information.

The authentication unit 321B, upon receiving authentication-instruction information from the history information recording unit 353B via the input/output unit 340B, acquires the history information 404 as first history information, and the history information 403 as second history information. Then, the authentication unit 321B judges whether the latest mounting was performed within a predetermined time period, with use of date/time items in the acquired pieces of

history information. Since the difference is 5 minutes in this case, the authentication unit 321B judges whether the mounting for the both times was performed at the same position. Since the positions of mounting are the same in this case, therefore the authentication unit 321B does not accept an input password, and instead, the process unit 322B sets access right and the like with use of the process information having been acquired last time and retained thereafter, so that the process is made accessible.

3.5 Summary of the third embodiment

As described above, the recording-medium unauthorized use prevention system 3 has, within the recording medium 300B, an authentication unit 321B that is tamper-resistant. This makes it difficult for third parties to encode or tamper the authentication system of the authentication unit. Therefore, it prevents unauthorized third parties from accessing the recording medium 300B.

In addition, the recording medium 300B detects mounting of itself to the portable telephone 100B, and once it is removed from the portable telephone 100B, the recording medium 300B requires the user to input the input password and the user information, if it is re-mounted after a predetermined time has passed, or if the position of mounting differs from last time. According to this, even when a third party has removed the recording medium 300B from the portable telephone 100B,

this person has to input the input password and the user information, if the recording medium 300B is re-mounted after a predetermined time has passed, or if the position of mounting differs from last time. This makes the recording medium 300B more difficult to be subject to unauthorized use, than conventionally.

4. Other modification examples

As described above, the recording medium includes therein an authentication unit that is tamper-resistant. This makes it difficult for third parties to encode or tamper the authentication system of the authentication unit. According to this, the recording medium is more effective in preventing third parties from using the recording medium, than conventional recording media.

In addition, the recording medium stores thereon one or more pieces of authentication information, and further one or more pieces of process information that each correspond to a piece of authentication information. Therefore, the user can use appropriate user information according to functions he wants to use. This makes it possible to restrict use of functions stored in this recording medium. Accordingly, this recording medium is more effective in preventing unauthorized use thereof by third parties, than conventional recording media.

In addition, the recording medium stores thereon one or

more pieces of communication information, and further one or more pieces of process information that each correspond to both of a piece of communication information and a piece of authentication information. Therefore, the user can use appropriate user information according to functions he wants to use. This makes it possible to restrict use of functions stored in this recording medium. Accordingly, this recording medium is more effective in preventing unauthorized use thereof by third parties, than conventional recording media. In addition, since the recording medium is operable to store thereon a plurality of pieces of communication information, the user does not have to carry a plurality of recording media, unlike conventional SIM cards. This reduces possibility of unauthorized use incident to loss or robbery.

In addition, the recording medium can detect mounting of itself to the portable telephone, and once it is removed from the portable telephone, the recording medium requires the user to input the input password and the user information, if it is re-mounted after a predetermined time has passed, or if the position of mounting differs from last time. According to this, even when a third party has removed the recording medium from the portable telephone, this person has to input the input password and the user information, if the recording medium is re-mounted after a predetermined time has passed, or if the position of mounting differs from last time. This makes the

recording medium more difficult to be subject to unauthorized use, than conventionally.

So far, the present invention has been described based on the aforementioned embodiments; however, needless to say, the present invention is not limited to the aforementioned embodiments, and includes the following examples.

(1) In the aforementioned description, the recording-medium unauthorized use prevention system has a portable telephone to which a recording medium is mountable. However, the present invention is not limited to such structure, and may have any kind as long as it is a terminal device to which a recording medium is mountable. Such terminal devices include a PDA (personal digital assistant), a personal computer, a car navigation system, a facsimile machine, and a digital camera.

(2) In the aforementioned description, user information is received from the portable telephone. However, the present invention is not limited to such structure, and may be a structure in which a recording medium is equipped with a fingerprint input unit, from which fingerprint information is received.

(3) In the present invention, the authentication information may be one of character information, biological information that represents biological characteristics of the user, and a combination of character information and biological information. Accordingly, the user information may also be

one of character information, biological information that represents biological characteristics of the user, and a combination of character information and biological information. Furthermore, in the third embodiment, input password and the registration password may also be one of character information, biological information that represents biological characteristics of the user, and a combination of character information and biological information.

Here, the biological information is, for example, fingerprint information, voice print information that represents characteristics of voice print of the user, iris information that represents characteristics of iris of the user, face-outline information that represents characteristics of face-outline of the user, DNA information that represents characteristics of DNA of the user, and a combination of some of the aforementioned information.

So as to accept voice print information, the portable telephone has to have a voice print input unit that receives voice of the user and generates voice print information of the user, using the received voice. So as to accept iris information, the portable telephone has to have an iris input unit that reads the iris of the user and generates iris information of the user, using the read iris. Likewise, so as to accept face-outline information, the portable telephone has to have a face-outline input unit that reads the face-outline of the user and generates

face-outline information of the user, using the read face-outline; and so as to accept DNA information, the portable telephone has to have a DNA-information input unit that accepts DNA information resulting from analyzing the DNA of the user. Here, the DNA information is analytical information on such as hair, blood, and saliva of the user.

Note here that matching of authentication information with the voiceprint information received at the recording medium happens when at least 80% of the received voiceprint information matches authentication information. The same thing applies to matching of authentication information with the iris information, matching of authentication information with the face-outline information, matching of authentication information with the DNA information. The reference value 80% may be other value. Matching of authentication information with a combination of some of the aforementioned information happens when all the information included in the authentication information matches all the information included in the combination of information.

(4) In the present invention, user information may be encrypted before being outputted from the portable telephone to the recording medium.

An example operation performed in this case is shown as follows.

A common key is owned by the portable telephone and the

recording medium. The portable telephone encrypts inputted user information using the common key, and outputs the encrypted user information to the recording medium; and the recording medium decrypts the encrypted user information using the common key, to obtain the user information inputted from the portable telephone.

(5) In the aforementioned description, the first storage area is set in the recording medium. However, the present invention is not limited to this structure, and the first storage area may be set in the portable telephone.

Furthermore, the second storage area set in the recording medium may be set in the portable telephone.

Likewise, the third storage area set in the recording medium may be set in the portable telephone.

Likewise, the password storage area set in the recording medium may be set in the portable telephone.

Likewise, the process unit set in the recording medium may be set in the portable telephone.

(6) In the aforementioned description, registration performed at the setting unit is operated through an external device. However, the present invention is not limited to such structure, and another structure is also possible in which registration is performed through a network such as the Internet to which the portable telephone is connected.

(7) In the aforementioned description, the setting unit

is used to register each piece of information to the storage area. However, the present invention is not limited to such structure, and another structure is also possible in which the setting unit performs modification and deletion of already registered information, not only registration.

The following describes how modification and deletion are performed to the authentication information and the process information of the first embodiment. In modifying authentication information, the recording medium receives, from an external terminal, the authentication number that corresponds to the authentication information to be modified, together with the authentication information after modified, and updates the authentication information table with use of the received pieces of information. In deleting authentication information, the recording medium receives from an external terminal the authentication number to be deleted, deletes the authentication information using the received authentication number, and further deletes the process information that corresponds to the deleted authentication information. In modifying process information, the recording medium receives, from an external terminal, the process number that corresponds to the process information to be modified, together with the process information after modified, and updates the process information table with use of the received pieces of information. In deleting process information, the recording medium receives

from an external terminal the process number to be deleted, and deletes the process information using the received process number, and further deletes the authentication information that corresponds to the deleted process information.

Next, the following describes how modification and deletion are performed to the authentication information, the communication information, and the process information, of the second and third embodiments.

In modifying authentication information, the recording medium receives, from an external terminal, the authentication number that corresponds to the authentication information to be modified, together with the authentication information after modified, and updates the authentication information table with use of the received pieces of information. In deleting authentication information, the recording medium receives from an external terminal the authentication number to be deleted, deletes the authentication information using the received authentication number, and further deletes the process information that corresponds to the deleted authentication information.

In modifying communication information, the recording medium receives, from an external terminal, the communication number that corresponds to the communication information to be modified, together with the communication information after modified, and updates the communication information table with

use of the received pieces of information. In deleting communication information, the recording medium receives from an external terminal the communication number to be deleted, and deletes the communication information using the received communication number, and further deletes the process information that corresponds to the deleted communication information.

In modifying process information, the recording medium receives from an external terminal a set of first number and second number that corresponds to the process information to be modified, together with the process information after modified, and updates the process information table with use of the received pieces of information. In deleting process information, the recording medium receives from an external terminal the set of first number and second number to be deleted, and deletes the process information using the received set of first number and second number.

(8) In the aforementioned description, the process name of process information to be registered in the second storage area is the process name owned by the recording medium. However, the present invention is not limited to such, and the process name of process information to be registered in the second storage area may be the process name owned by the portable telephone.

(9) In the aforementioned description, the recording-medium unauthorized use prevention system comprises

a portable telephone and a recording medium. However, the present invention is not limited to such structure, and the system may comprises only a portable telephone. In this case, each process that corresponds to the process information to be registered in the second storage area may be set in a recording medium located inside the portable telephone, or may be set in a recording medium that can be mounted to the portable telephone, or may be set in both of them.

In this case, one example of the timing when the judgment should be performed as to whether to receive an input password is as follows. That is, the portable telephone detects every time power supply starts to the portable telephone, and stores the detected timing as history information. The judgment whether to receive an input password is performed with use of this history information. Or, the password may be received every time the starting of power supply is detected.

(10) The operation for setting authentication information and process information, which is shown in the first embodiment, is not limited to the flowchart of FIG. 6. Another structure is also possible in which process information is set first, and then authentication information is set.

An example of operation for this case is described as follows. The recording medium receives from an external terminal process information to be registered, then calculates a process number, and with use of the calculated process number,

sets the received process information. Next, the recording medium receives from an external terminal, authentication information to be registered, and judges whether the received authentication information has been already registered. If the received authentication information has not yet been registered, the process number calculated in the setting of the process information is used as an authentication number, and the recording medium performs authentication information setting with use of this authentication number and the received authentication information. If the received authentication information has been already registered, different authentication information is received and setting operation therefor is performed.

(11) In the second embodiment, a telephone number is stored as communication information. However, the present invention is not limited to such; another structure is possible in which a telephone number is encrypted using a function, and the encrypted information is stored. In performing communication, the encrypted information is transmitted to the base station. An example of encryption method is stream cipher.

According to the structure in which a telephone number is stored after being encrypted using a function, any third party is prevented from easily knowing the telephone number, even if this person has acquired the communication information stored in the third storage area 313A. This prevents

unauthorized use by third parties.

Here, the function used in encryption of a telephone number may be stored in the recording medium, or may be retained by an agent who provides the portable telephone with communication functions through the communication information.

Or, in advance, the owner of the communication information may convert a telephone number into information that only he can know. In this case, too, unauthorized use by third parties is prevented.

In this case, list information may be generated with use of the communication information stored in the communication information table, as it is. Or the encrypted information may be decrypted first, then list information is generated with use of the decrypted information.

Or, the communication information table may be provided with an item for registering therein such encrypted information in correspondence with a telephone number. In this structure, a registered telephone number is used in generating list information, and encrypted information corresponding to the selected telephone number is used in communication.

Or, it is possible to register encrypted information in the communication information item of the communication information table, and to have a new table in which encrypted information is stored in correspondence with information before encryption, and to use this new table in generation of list

information.

(12) Registration into each storage area described in the second embodiment is not limited to the order shown in FIG. 15, and may be in any order.

(13) In the second embodiment, a plurality of pieces of communication information are stored in the communication information table. However, the communication information table may have only one piece of communication information.

In this case, the process information is stored in the second storage area, after being associated with both of the communication information and the authentication information that has been registered in the second storage area. When user information is inputted in authentication, authentication information that corresponds to the inputted user information is recognized, and process information corresponding to both of the authentication information and the communication information is acquired, and the process for the process name registered in the acquired process information is made accessible.

At this time, the selection unit may be eliminated from the structure, and that the process unit may always read communication information from the third storage area.

(14) In the second embodiment, "N.A." as communication information which indicates that no communication information is necessary may be registered in the communication information

table. In this case, process information is registered in association with the set of the communication information "N.A." and the corresponding authentication information. Note here that in setting process information, the process information setting unit has to control to disable setting of a communication function to the set of the communication information "N.A." and the corresponding authentication information.

(15) In the third embodiment, judgment as to whether an input password should be received is affirmative, either when the difference in date/time is no smaller than a predetermined value, or when the difference in position is no smaller than a predetermined value. However, the present invention is not limited to such; and the judgment may be affirmative when the difference in date/time is no smaller than a predetermined value, and the difference in position is no smaller than a predetermined value.

In addition, judgment as to whether an input password should be received is based on both of date/time information and position information. However, the present invention is not limited to such. Only one of date/time information and position information may be used in the judgment. Or, it is also possible to structure so as to request an input password every time the mounting of the recording medium to the portable telephone is detected. In this case, the authentication unit may request the portable telephone to input the input password,

upon receiving from the history information recording unit an instruction to start authentication.

Or, the input password reception may be omitted. In this case, when the mounting of the recording medium to the portable telephone is detected, judgment as to whether authentication is required may be performed using the first history information and the second history information, and if the judgment is affirmative, communication information to be used and user information are accepted, and authentication is performed. Or, it is also possible to structure so that communication information to be used and user information are accepted, every time the mounting of the recording medium to the portable telephone is detected. Here, if authentication should be performed according to a user instruction, it is only required that the recording medium request the portable telephone to input communication information and authentication information, upon receiving authentication-start information from the portable telephone.

(16) In the authentication in the third embodiment, the operation is not limited to as shown in the flowchart of FIGs. 23 and 24. For example, if the recording medium is mounted to the portable telephone within the predetermined time period, and that at the same position, the operation from Step S430 may be performed.

(17) In the third embodiment, registration of history

information may be performed at regular time intervals. In this case, the history information recording unit owns a timer function for setting a time at which history information is written regularly. After history information is written and the time set in the timer function has elapsed, judgment is performed as to whether a mounting-detect signal is received from the detection unit. If receiving a mounting-detect signal, the recording medium acquires date/time information and position information from the portable telephone, and with use of the acquired pieces of information, generates history information, and registers the generated history information to the history information table. For this, category information of the history information may be "mounting", or may be information indicating that the registration of history information is performed by a regular inspection, such as "regular".

In addition, after registration of history information, the registered history information is compared with the history information registered last time, for judging whether an input password should be received. If the judgment is affirmative, an input password is received, and correctness of the user is judged. If the user is judged to be a correct user, the operation from Step S430 in FIG. 23 may be performed. Or, only judgment as to the correctness of the user may be performed, and as for the accessible processes, the already stored information may

continue to be used. In this case, comparison of history information may be performed using only the position information.

(18) Steps S70 - S83 of the first embodiment shown in FIG. 7 are not essential steps. If there is no authentication information that matches the received user information, the steps after Step S70 may be omitted, or even Step S70 and thereafter may be omitted.

Furthermore, in FIG. 16 which is for the second embodiment, steps S225 - S250 are performed when there is no authentication information that matches the received user information. However, the present invention is not limited to this. If there is no such authentication information, the steps after Step S225 may be omitted, or even Step S225 and thereafter may be omitted. Furthermore, Step S250 is not essential, and may be omitted.

Furthermore, in FIG. 23 which is for the third embodiment, Step S425 is not essential and may be omitted. Furthermore in FIG. 24, if there is no authentication that matches the received user information, Steps S455 to S480 are performed. However, the present invention is not limited to such, and the steps after Step S455 may be omitted, or even Step S455 may be omitted. In addition, Step S480 is not essential and may be omitted.

(19) At Step S75 of FIG. 7 which is for the first embodiment,

if there is no authentication-unnecessary number, the operation ends there. However, the present invention is not limited to such. If there is no authentication-unnecessary number, the process-in-use information stored in the process-name storage area may be used to control so that the process of the process name registered in the process-in-use information is made inaccessible.

In addition, if there is no authentication information at Step S55, it is also possible to perform Step S70, then control so that the process for the process name registered in the process-in-use information is made inaccessible with use of the process-in-use information stored in the process-name storage area, then end the operation. Or, only the aforementioned control may be performed.

(20) Likewise, at Step S230 of FIG. 16 which is for the second embodiment, if there is no authentication-unnecessary number, control may be performed so that the process for the process name registered in the process-in-use information is made inaccessible, with use of the process-in-use information stored in the process-name storage area.

In addition, if there is no authentication information at Step S215, it is also possible to perform Step S225, then control so that the process for the process name registered in the process-in-use information is made inaccessible with use of the process-in-use information stored in the process-name

storage area, then end the operation. Or, only the aforementioned control may be performed.

In addition, at Step S240 of FIG. 16 which is for the second embodiment, if there is no process information, a message is outputted then the authentication operation ends. But the present invention is not limited to such, and another structure is also possible in which a message is outputted, and control is performed so that the process for the process name registered in the process-in-use information is made inaccessible with use of the process-in-use information registered in the process-name storage area, and the operation ends. Or, if there is a set of first number and second number that corresponds to the set of the communication number acquired at the selection unit and the authentication-unnecessary number, access right is set to the process for the process name registered in the process information that corresponds to the aforementioned set of first number and second number, so as to make the process accessible.

Furthermore, if there is no set of first number and second number that corresponds to the communication number and the authentication-unnecessary number, the following operation may be performed.

If there is a set of first number and second number that corresponds to a set of communication number that corresponds to the communication information "N.A." and the

authentication-unnecessary number, access right is set to the process for the process name registered in the process information that corresponds to the set of first number and second number, so that the process is made accessible. If there is no such set of first number and second number, control is performed so that the process for the process name registered in the process-in-use information is made inaccessible, with use of the process-in-use information stored in the process-name storage area, then the operation ends.

(21) At step S420 of FIGs. 23 and 24 for the third embodiment, if the password is judged not to be correct, a message is outputted and the authentication operation ends. However, the present invention is not limited to this. Another structure is also possible in which, after a message is outputted, control is performed so that the process for the process name registered in the process-in-use information is made inaccessible with use of the process-in-use information stored in the process-name storage area, then the operation ends.

In addition, at Step S460, the same operation may be performed as that performed at Step S230 in the aforementioned modification example (20). At Step S445, the same operation may be performed as that performed at Step S215 in the aforementioned modification example (20). In addition, at Step S470, the same operation may be performed as that performed at Step S240 in the aforementioned modification example (20).

(22) In the aforementioned modification examples (19), (20), and (21), in controlling so that the process for the process name registered in the process-in-use information is made inaccessible, the process-in-use information stored in the process-name storage area may be deleted after the process has been made inaccessible, so that there will be nothing stored in the process-name storage area.

(23) In the first embodiment, the storage area has two tables: an authentication information table and a process information table. However, not limited to such, the first embodiment may have a structure in which the storage area has only one table that has both authentication information and process information in correspondence.

Here, one example of such a table is shown in FIG. 26. Each item therein is the same as that in the first embodiment, therefore will not be detailed here.

Likewise, in the second and third embodiments, the storage area has an authentication information table, a process information table, and a communication information table. However, not limited to such, the three tables may be integrated into one table.

Here, one example of such a table is shown in FIGs. 27 and 28. FIG. 27 has only one piece of communication information, and FIG. 28 has a plurality of pieces of communication information. Each item therein is the same as those in the second and third

embodiments, therefore will not be detailed here.

(24) As for the communication function described in the second and third embodiments, each function to be included therein such as a calling function, an electric mail function, and a call-reception function, may be registered individually. Or, a communication number and an authentication number may be corresponded to the content of the function. Further, it is possible to set a limit for the calling bill in using the communication function, so as to correspond a communication number and an authentication number, to the limit.

Furthermore, in the electronic commerce function, a communication number and an authentication number may be set according to the goods to be dealt with, or to the prices thereof.

Furthermore, in the second and third embodiments, functions that users can use are a memory function, a game function, a communication function, and an electronic commerce function. However, not limited to such, the functions may include others as long as they are accessible through the recording medium.

For example, it is possible to include an electric money function therein, and accordingly include "electric money function" in the process information table as process information item. At that time, it is possible to set a communication number and an authentication number for each function included in the electric money function, such as saving,

balance-inquiry, and withdrawal.

Furthermore, it is possible to include a navigation function therein, and accordingly include "navigation function" in the process information table as process information item.

In addition, in the first embodiment, the processes that the user can use are the memory A, the memory B, and the game. However not limited to such, the processes may include others as long as they are accessible through the recording medium.

In addition, in the first, second, and third embodiments, the functions accessible to the user that are stored in the storage area of the recording medium have been prestored at the time of purchase of the recording medium. However, not limited to such, the functions may be registered in the storage area at the time of setting the purchase information after the purchase.

(25) The present invention only permits use of the process for the process name acquired in authentication. However, not limited to such, the present invention may have a structure of including processes whose process names are acquired at the time of authentication, as processes that are allowed to be used, in addition to the processes that have been allowed to be used prior to starting of the authentication.

The following shows one example of a realization method in a case when process information storing process names corresponds to authentication information. The recording

medium receives from the portable telephone process-add information that instructs to add processes to be allowed. Upon receiving the process-add information, the recording medium requests the portable telephone to input user information. The recording medium acquires an authentication number of the authentication information that matches the user information received from the portable telephone, and acquires process information that corresponds to the acquired authentication number. Then, the process whose process name has been registered in the acquired process information will be allowed to be used.

The following shows one example of a realization method in a case when process information storing process names corresponds to a set of communication information and authentication information. The recording medium stores therein the communication number selected in the last authentication. The recording medium, upon receiving process-add information from the portable telephone, requests the portable telephone to select communication information, then judges whether the communication information received from the portable telephone matches the communication information selected in the last authentication. If the two pieces of communication information are judged to match each other, the recording medium requests the portable telephone to input user information. The recording medium then acquires an

authentication number for the authentication information that matches the user information received from the portable telephone, and acquires process information that corresponds to the set of the acquired authentication number and a communication number. Then, the process whose process name has been registered in the acquired process information will be allowed to be used. If the two pieces of communication information are judged not to match each other, the operation ends there.

(26) In the third embodiment, date, time, and minute are used to show the time of mounting in history information. However, date, hour, minute, and second may be used therefor.

Moreover, the predetermined time interval prestored in the recording medium is 30 minutes. However, not limited to such, it may be other time intervals. In addition, the time interval may be in a unit of any one of hour, minute, and second.

In addition, an external terminal is used to register a predetermined time interval that is to be prestored in the recording medium. However, the registration may be performed from the portable telephone.

In addition, the position information is registered as the history information in a unit of municipalities. However, the value of its longitude and latitude may be used in registration. At this time, judgment as to whether the positions of mounting of the recording medium to the portable

telephone are the same is based on the value of longitude and latitude of this time and the value of last time. If there is no difference therebetween, the positions may be judged to be the same. Or, it is also possible to calculate a distance of moving with use of the value of longitude and latitude of this time and the value of last time, and to judge that the positions are the same if the distance of moving is within a predetermined distance. In this case, the recording medium has to prestore the value of distance of moving that is to be considered the same position of mounting.

(27) In the present invention, the reference value which is the basis of judgment as to whether the fingerprint information matches the authentication information is 80%; however other reference values may be used.

(28) In the present invention, the process for the process name that corresponds to the authentication-unnecessary number (hereinafter "authentication-unnecessary process") is allowed when there is no authentication information that matches the user information received in authentication. However, not limited to this, the recording medium may allow use of an authentication-unnecessary process when receiving from the portable telephone information instructing to use the authentication-unnecessary process.

In the following, an example of a realization method in this case is described with use of the first embodiment. The

recording medium, upon receiving authentication-start information, outputs, to the portable telephone, information for inquiring about whether an authentication-unnecessary process should be used. The recording medium then judges whether information received from the portable telephone is information instructing to use an authentication-unnecessary process. If the information is judged to instruct to use an authentication-unnecessary process, the recording medium permits use of the authentication-unnecessary process; and if the information is judged not to instruct to use an authentication-unnecessary process, the recording medium outputs input-means information to the portable telephone. The operations hereafter are the same as those of the first embodiment, therefore will not be detailed here.

(29) In the present invention, it is also possible to enable use of an authentication-unnecessary process every time the recording medium is mounted to the portable telephone.

(30) In the present invention, the recording medium receives user information, and then permits use of a process that corresponds to authentication information that matches the received user information. However, the procedure is not limited to such, and it is also possible to have a procedure in which process information for the process that the user wants to use is received, and after that, the corresponding authentication information is received, which is then used for

authentication.

The following shows one example of a realization method in a case when the process information corresponds to authentication information.

After receiving authentication-start information, the recording medium outputs to the portable telephone a list of process information registered in the process information table. The portable telephone, upon receiving the list of process information, displays the received list of process information, receives from the process information of his choice, and outputs the received process information to the recording medium. The recording medium acquires the authentication number that corresponds to the received process information, and judges whether the acquired authentication number is an authentication-unnecessary number. If it is judged to be an authentication-unnecessary number, the recording medium permits use of the process corresponding to the process information received from the portable telephone, without performing authentication. If it is judged not to be an authentication-unnecessary number, the recording medium requests the portable telephone to input user information that corresponds to the content of the authentication information for the acquired authentication number, then receives input of user information from the portable telephone. For example, if the content of the authentication information that

corresponds to the acquired authentication number is fingerprint information, the recording medium requests input of fingerprint information; if the content thereof is character information, the recording medium requests input of character information; and if the content thereof is both of character information and fingerprint information, the recording medium requests input of both of character information and fingerprint information.

The following shows one example of a realization method in a case when the process information corresponds to communication information and authentication information.

After receiving authentication-start information, the recording medium further receives number-to-be-used information from the portable telephone. Next, the recording medium outputs to the portable telephone a list of process information registered in the process information table, and performs the procedure described above.

(31) In the present invention, use of a process is allowed at the time of authentication by setting access right to the process for the acquired process name. However, not limited to this, it is also possible to control in the following way. In advance, all the processes whose process name is registered in the process information are assigned access right so that they are accessible. The recording medium acquires process information according to the authentication content. After

authentication, the recording medium receives, from the portable telephone, information instructing use of the process, judges whether the process to be used is a process whose process name has been registered in the process information acquired in authentication, and enables use of the process if the judgment is affirmative.

(32) In the present invention, if there are more than a piece of authentication information that match a received piece of user information, it is possible to set access right to the corresponding number of processes, whose process names have being registered in pieces of process information that each correspond to each of the pieces of authentication information.

To explain the above, an example is taken where the recording medium has two pieces of fingerprint information taken from the same finger (hereinafter "first fingerprint information" and "second fingerprint information"). In this case, if the fingerprint information received in authentication matches both of the first fingerprint information and the second fingerprint information, the authentication unit permits use of both of the process for the process name registered in authentication information that corresponds to the first fingerprint information, and the process for the process name registered in authentication information that corresponds to the second fingerprint information.

(33) The present invention may be the methods described above. Furthermore, these methods may be a computer program that enables such method using a computer. Moreover the present invention may be a digital signal comprised of the computer program.

In addition, the present invention may be a computer-readable recording medium such as a flexible disk, a hard disk, a CD-ROM, an MO, a DVD, a DVD-ROM, a DVD-RAM, a BD(Blu-ray Disc), and a semiconductor memory, that records thereon the aforementioned computer program or the digital signal. Or, the present invention may be the aforementioned computer program or the digital signal, recorded on these recording media.

In addition, the present invention may be the aforementioned computer program or the digital signal, transmitted through a network and the like, represented by an electric communication circuit, a radio circuit, a cable communication circuit, and the Internet.

Furthermore, the present invention may be a computer system equipped with a microprocessor and a memory, where the memory stores thereon the aforementioned computer program, and the microprocessor performs according to the aforementioned computer program.

In addition, the present invention may be executed by an independent another computer system, by transmitting the

aforementioned program or the digital signal recorded on the recording medium, or by transmitting the aforementioned program or the digital signal through the aforementioned network and the like.

(34) The present invention may be a combination of some of the described embodiments and the modification examples.

5. *Summary*

As described in the above sections, the present invention is a system of preventing unauthorized use of a recording medium which is mountable to a terminal device ("recording-medium unauthorized use prevention system"). This recording-medium unauthorized use prevention system is characterized by having a first storage area, a second storage area, an authentication unit, and a process unit, the first storage area storing thereon a plurality of pieces of authentication information used in determining whether use of the recording medium should be allowed, the second storage area storing thereon process means corresponding to the authentication information stored in the first storage area, the authentication unit performing authentication with use of the authentication information and user information that the owner of the recording medium has, and the process unit executing the process means according to the content of authentication performed by the authentication unit.

Here, the system may further have a third storage area for storing thereon communication information for using the communication function of the terminal device, and the process unit may execute the process means that corresponds to the communication information and the authentication content of the authentication unit.

Here, the system may further have a fourth storage area for storing thereon a plurality of pieces of communication information, and a selection unit that selects a piece of communication information that the user desires, and the process unit may execute the process means that corresponds to the communication information selected by the selection unit and the authentication content of the authentication unit.

Here, the system may further have a detection unit that detects mounting/dismounting of the recording medium to/from the terminal device, and authentication by the authentication unit may be performed, if the recording medium is to be used again after the detection unit has detected dismounting of the recording medium from the terminal device.

Here, the system may further have an authentication-information setting unit that sets the authentication information, and the authentication information set by the authentication-information setting unit may be stored in the first storage area.

Here, the system may further have a process-means setting

unit that sets the process means, and the process means set by the process-means setting unit may be stored in the second storage area.

Here, the system may further have a communication-information setting unit that sets the communication information, and the communication information set by the communication-information setting unit may be stored in the third or fourth storage area.

Moreover, the present invention is a recording medium that is used in the system and is mountable to a terminal device. This recording medium is characterized by including at least a first storage area and a second storage area, the first storage area storing thereon a plurality of pieces of authentication information used for determining whether the recording medium can be used, and the second storage area storing thereon pieces of process means that are in correspondence with the pieces of authentication information.

Here, the recording medium may further have a third storage area storing thereon communication information for using the communication function of the terminal device.

Here, the recording medium may further have a fourth storage area storing thereon a plurality of pieces of communication information for using the communication function of the terminal device.

Here, the recording medium may further have an

authentication unit that performs authentication using the authentication information and user information that the owner of the recording medium has.

Here, the recording medium may further have a detection unit that detects mounting/dismounting of the recording medium to/from the terminal device, and authentication by the authentication unit may be performed, if the recording medium is to be used again after the detection unit has detected dismounting of the recording medium from the terminal device.

In addition, the present invention is a terminal device which is used in the system and to which a recording medium is mountable. This terminal device is characterized by having at least a first storage area, a second storage area, an authentication unit, and a process unit, the first storage area storing thereon a plurality of pieces of authentication information used in determining whether use of the recording medium should be allowed, the second storage area storing thereon process means corresponding to the authentication information stored in the first storage area, the authentication unit performing authentication with use of the authentication information and user information that the owner of the terminal device has, and the process unit executing the process means according to the content of authentication performed by the authentication unit.

Here, the terminal device may further have a fourth storage

area storing thereon a plurality of pieces of communication information for using the communication functions of the terminal device, and a selection unit that selects a piece of communication information that the user desires out of the pieces of communication information stored in the fourth storage area.

In addition, the present invention is a method of preventing unauthorized-use of a recording medium that is mountable to a terminal device. This unauthorized-use prevention method is characterized by having: a first storing step of storing a plurality of pieces of authentication information for determining whether use of the recording medium should be allowed; a second storing step of storing process means corresponding to the authentication information; an authentication step of performing authentication with use of the authentication information and user information that the owner of the recording medium has; and a process step of executing the process means according to the content of authentication performed at the authentication step. Furthermore, the present invention is a recording-medium unauthorized use prevention system for executing this method.

Furthermore, the present invention is a method of preventing unauthorized-use of a recording medium that is mountable to a terminal device. This method is characterized by having: a first storing step of storing a plurality of pieces of authentication information for determining whether use of

the recording medium should be allowed; a second storing step of storing pieces of process means corresponding to the pieces of authentication information; a third storing step of storing communication information for using the communication function of the terminal device; an authentication step of performing authentication with use of the authentication information and user information that the owner of the recording medium has; and a process step of executing the process means according to the communication information and the content of authentication performed at the authentication step.

Furthermore, the present invention is a recording-medium unauthorized use prevention system that executes this method.

Furthermore, the present invention is a method of preventing unauthorized use of a recording medium that is mountable to a terminal device. This method is characterized by having: a first storing step of storing a plurality of pieces of authentication information for determining whether use of the recording medium should be allowed; a second storing step of storing pieces of process means corresponding to the authentication information; a fourth storing step of storing a plurality of pieces of communication information for using the communication function of the terminal device; a selection step of selecting a piece of communication information that the user desires out of the pieces of communication information stored at the fourth storing step; an authentication step of

performing authentication with use of the authentication information and user information that the owner of the recording medium has; and a process step of executing the process means according to the piece of communication information selected at the selection step and the content of authentication performed at the authentication step. Furthermore, the present invention is a recording-medium unauthorized use prevention system that executes this method.

6. *The effects of the present invention*

As described in the above, the present invention is a portable recording medium characterized by including: a storage unit which stores therein storage authentication information that authenticates a user, and has an area that corresponds to the storage authentication information; a judgment unit operable to judge whether to perform authentication; a reception unit operable to receive reception authentication information that authenticates a user, if the judgment unit judges affirmative; an authentication unit that is tamper-resistant and is operable to judge whether the received reception authentication information matches the storage authentication information; and a process unit operable to permit use of the area if the reception authentication information is judged to match the storage authentication information.

According to the stated structure, the recording medium has an authentication unit that is tamper-resistant. Because of being tamper-resistant, the authentication unit is prevented from being decoded or tampered by third parties. According to this, the recording medium prevents unauthorized use of areas included therein by third parties.

Here, the storage unit may further store therein other storage authentication information different from the storage authentication information, and have another area that corresponds to the other storage authentication information, the authentication unit, instead of judging whether the received reception authentication information matches the storage authentication information, may judge whether the received reception authentication information matches the storage authentication information, and judge whether the received reception authentication information matches the other storage authentication information, and the process unit may further permit use of the other area, if the reception authentication information is judged to match the other storage authentication information.

According to the stated structure, the recording medium stores thereon other storage authentication information different from the storage authentication information, and has another area that corresponds to the other storage authentication information, and so it becomes possible to permit,

if the received reception authentication information is judged to match the storage authentication information, use of the area corresponding thereto, and to permit, if the received reception authentication information is judged to match the other storage authentication information, use of the other area corresponding thereto.

Here, the recording medium may further include a detection unit operable to detect that the recording medium is mounted to a terminal device, where the judgment unit may judge that authentication is to be performed, after the detection unit has detected the mounting.

According to the stated structure, the recording medium is able to judge to perform authentication if the mounting thereof to an external device is detected.

Here, the recording medium may further include a recording unit operable to record, when the detection unit has detected the mounting, first history information that indicates the mounting, the recording unit recording in advance second history information that indicates another mounting that occurred prior to the mounting, where the judgment unit may judge whether to perform authentication, using the first history information and the second history information.

According to the stated structure, the judgment unit is able to perform judgment whether to perform authentication, with use of the first and second history information.

Here, the first history information may have first date/time information that shows date and time in which the mounting is detected, the second history information may have second date/time information that shows date and time in which the other mounting is detected, and the judgment unit may judge that authentication is to be performed, if a difference in date and time between the first date/time information and the second date/time information is no smaller than a predetermined value.

According to the stated structure, the judgment unit is able to judge to perform authentication, if the difference in date and time is no smaller than a predetermined value.

Here, the first history information may have first position information that shows a position at which the mounting is detected, the second history information may have second position information that shows a position at which the other mounting is detected, and the judgment unit may judge that authentication is to be performed, if a difference in position between the first position information and the second position information is no smaller than a predetermined value.

According to the stated structure, the judgment unit is able to judge to perform authentication, if the difference in position is no smaller than a predetermined value.

Here, the storage authentication information may be one

of first character information, first biological information, and first combination information, the first character information comprising at least one number, letter, and symbol, the first biological information showing biological characteristics of the user, and the first combination information comprising first character information and first biological information, the reception authentication information may have second character information, second biological information, and second combination information, the second character information comprising at least one number, letter, and symbol, the second biological information showing biological characteristics of the user, and the second combination information comprising second character information and second biological information, and the authentication unit, when the received reception authentication information is the second character information, may judge whether the second character information matches the first character information, and when the received reception authentication information is the second biological information, judge whether the second biological information matches the first biological information, and when the received reception authentication information is the second combination information, judge whether all information included in the second combination information matches all information included in the first

combination information.

According to the stated structure, the authentication unit is able to perform judgment as to one of: whether the first character information matches the second character information; whether the first biological information matches the second biological information; and whether the first combination information matches the second combination information.

Here, the first biological information and the second biological information may be one of fingerprint information, voice print information, iris information, face-outline information, and DNA information, the fingerprint information showing characteristics of the user's fingerprint pattern, the voice print information showing characteristics of the user's voice print, the iris information showing characteristics of the user's iris, the face-outline information showing characteristics of outline of the user's face, and the DNA information showing characteristics of the user's DNA.

According to the stated structure, the first biological information and the second biological information may be one of fingerprint information, voice print information, iris information, face-outline information, and DNA information.

Here, the recording medium may be assigned a telephone number that the terminal device uses in communication, the storage unit may further store therein communication

information that represents the telephone number, the area may further correspond to the communication information, and the process unit may further permit use of the area that corresponds to the communication information.

According to the stated structure, the area of the storage unit is further be corresponded to communication information, and the process unit is further able to permit use of the area corresponded to the communication information.

Here, the recording medium may further include a selection unit operable to receive selection of the communication information, where the process unit may further permit use of the area that corresponds to the communication information selected through the selection unit.

According to the stated structure, the communication information is able to be selected by the selection unit, and the process unit is further able to permit use of the area corresponded to the communication information that has been selected through the selection unit.

Here, the recording medium may further include a setting unit operable to receive the storage authentication information and to write to the storage unit the received storage authentication information in correspondence with the area of the storage unit.

According to the stated structure, storage authentication information is able to be corresponded to the area of the storage

unit, before being stored.

Here, the setting unit may further receive communication information that represents a telephone number assigned to the recording medium, and write to the storage unit the received communication information in correspondence with the area.

According to the stated structure, the setting unit is further able to store communication information in correspondence with the area of the storage unit.

Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless otherwise such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.